Anomali Security Analytics

User Guide

July 9, 2026

Copyright

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

Documentation Updates

(**Limited Availability)

Date	Description
July 9, 2026	Updated information about the Mimecast Version 2.0 API that uses Client ID and Client Secret, replacing Version 1.0.
Oct 9, 2025	Added information about the informational status in the alert action menu.
Oct 3, 2025	Added information about the alert schema for alerts forwarded to Azure Sentinel.
Sep 26, 2025	Added information about the ability to attach a PDF to an email alert.
Aug 26, 2025	Removed information related to the deprecation of the Data Usage Dashboard

Aug 6, 2025	Added information about limitations regarding alerts that are sent to webhooks.
Jul 31, 2025	Added information about the origin column in the audit table.
Jul 30, 2025	Added information about critical alerts to assign higher priority to critical alerts.
Jul 16, 2025	Updated information about the supported log source parsers.
Jul 14, 2025	Added information about the Security Analytics Data Retention policy.
Jul 14, 2025	Added information about the ability to use API calls as a new method of log ingestion.
Jun 24, 2025	Added information about deprecating the Retrosearch API and using the Search jobs API along with turbosearch.
Jun 4, 2025	Added information about the ability to forward alert payloads to S3 when you create an search event alert.
May 5, 2025	Added information about log source management that allows users to ingest event telemetry data from various log sources using one or more ingestion methods.
Feb 20, 2025	Added information about adding an alert triage when user creates search event alerts.
Feb 12, 2025	Added information about dashboard actions now being auditable.
Feb 6, 2025	Added information about webhooks supporting custom JSON payloads when forwarding matches to third-party services

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 (Anomali Security Analytics)

- Send your feedback to support@anomali.com.

Thank you for your feedback!

CONTENTS

Chapter 1: Anomali Security Analytics Overview 19

Anomali Security Analytics Key Objectives 19

Anomali Security Analytics Deployment Components 20

Chapter 2: Using Anomali Security Analytics Dashboards 23

Getting Started with Dashboards 23

Panels 24

Time Period 25

Saved Search 27

Export CSV 27

Overview Dashboard 28

Matched Threat Models 30

Top 20 Impacted Hosts by Risk Score 32

Indicator Match Timeline 34

Matches by Threat Type 35

Top Originating Countries 36

Multi Dimensional Dashboard 38

Indicator Match Timeline 39

Top Matches By Source Host 40

Top 10 Destination Ports 42

Top Matches By Indicator 42

Indicator Matches by Action 43

Indicator Matches by iType 44

Indicator Matches by Severity 45

Indicator Matches by Confidence 46

Indicator Matches by Geo Location 47

Indicator Matches 48

Match Analysis Dashboard 49

Matches Over Time 51

Matches by Feed 51

Matches by iType 53

Matches by Indicator 54

Matches by DGA 55

Chapter 3: Searching Anomali Security Analytics Activity Databases 57

Getting Started with Activity Search 57
Activity Search Indexes 57
Full-Text Search 58
Keyword Search 59
Field-Based Search 59
Search Raw Events 62
Filter UI 63
Date Range Filter 64
Saved Searches 65
Search Result Fields 65
Export Search Results 66

IOC Match Activity Searches 68
About IOC Match Searches 68
Filter UI 69
Advanced Filter Expression Examples 71
Filter Operators 72
Filter Fields 72
IOC Match Results Table 90

DGA Match Activity Searches 94
About DGA Match Searches 95
Filter UI 95
Filter Examples 96
Filter Operators 97
Filter Fields 97
DGA Match Results Table 109

Actor Activity Searches 112
About Actor Searches 112
Filter UI 112
Filter Examples 114
Filter Operators 115
Filter Fields 115
Actor Match Results Table 118

Attack Pattern Activity Searches 122
About Attack Pattern Searches 123
Filter UI 124
Filter Examples 125

Filter Operators 126
Filter Fields 126
Attack Pattern Matches Results Table 130
Campaign Activity Searches 133
About Campaign Searches 134
Filter UI 134
Filter Examples 136
Filter Operators 137
Filter Fields 137
Campaign Matches Results Table 140
Threat Bulletin Activity Searches 144
About Threat Bulletin Searches 145
Filter UI 146
Filter Examples 147
Filter Operators 148
Filter Fields 148
Threat Bulletin Matches Results Table 151
TTP Activity Searches 155
About TTP Searches 156
Filter UI 157
Filter Examples 158
Filter Operators 159
Filter Fields 159
TTP Matches Results Table 163
Vulnerability Activity Searches 167
About Vulnerability Searches 167
Filter UI 167
Filter Examples 169
Filter Operators 170
Filter Fields 170
Vulnerability Matches Results Table 176
Alerts Activity Searches 180
About Alerts Searches 180
Filter UI 181
Filter Examples 181
Filter Operators 182
Filter Fields 182
Alerts Match Results Table 198

Asset Activity Searches 202
About Asset Searches 202
Filter UI 203
Filter Examples 205
Filter Operators 205
Filter Fields 206
Asset Match Results Table 208

Chapter 4: Managing Saved and Scheduled Configurations 215

Using Alerts 215
Triage your Alerts 220
Creating Alerts 220
Setting Alert Actions 241
Alert Triage 244
Managing Alerts 250

Managing Saved Searches 254
About Saved Searches 255
Issue a Saved Search 255
Modify a Saved Search 255
Delete a Saved Search Configuration 256
Create an Alert Based on a Saved Search 256

Managing Retrospective Search Jobs 256
About Retrospective Search Jobs 256
Schedule a Retrospective Search Job 257
Toggle Activation for a Retrospective Search Job Configuration 265
Modify a Retrospective Search Job Configuration 265
Clone a Retrospective Search Job Configuration 265
Delete a Retrospective Search Job Configuration 265
View Job History and Download Results 265
Troubleshooting 267

Managing Reports 268
Create a Scheduled Report Job 268
View Report Job History and Download Reports 270
Manage Report Configurations 271

Managing Exports 272
Download an Export 273
Delete an Export 273
View Export Job Status 273

Managing Exclude Lists 273
About Exclude Lists 273
Manage the Suppressed Indicators List 273
Manage the DGA Exclude List 276
Manage the Asset Exclude List 278
Manage the Suppressed iTypes List 279
Manage the Suppressed Feeds List 281
Managing Lookup Tables 283
Lookup Table Permissions 283
About Lookup Tables 283
Upload a Lookup Table 284
Append to an Existing Lookup Table 287
Update a Lookup Table 288
View a Lookup Table 289
Export a Lookup Table 289
Delete a Lookup Table 290

Chapter 5: Modifying My Profile 293
Change the Default Date Range Filter 293

Chapter 6: Managing Anomali Security Analytics Settings 295
Configuring General Settings 295
Modify DGA Settings 295
Modify Filter Settings 296
Modify My Data Settings 303
Managing Links and Log Sources 304
About Links 304
Monitor Link Health 306
Upgrade Link Software 308
Regenerate a Universal Link Configuration 314
Delete a Link Configuration 314
Manage Log Source Configurations 315
Managing Asset Data Imports 321
About Asset Data Sources 321
Managing Qualys Scanner Imports 322
Managing Rapid7 Scanner Imports 326
Managing Tenable Scanner Imports 329
Managing AWS Asset Data Imports 335
Managing Asset CSV File Imports 343

Adding Manual Entries 346
Managing Anomali Security Analytics Users 348
Modifying IOC Correlation Engine Settings 349
About the IOC Correlation Engine 349
Modify IOC Correlation Settings 352

Chapter 7: User and Role Management 353

Chapter 8: Audit Logging (Limited Availability) 355
Auditing Scope 355
Auditable Fields 356
Audit Logs for Analyzing Activity 361
Creating Dashboards for Audits 363
Audit Logs for User Actions 364
Alert Configuration Audit Logs 364
Saved Searches Audit Logs 364
Retrospective Searches Audit Logs 364
Report Management Audit Logs 365
Export Audit Logs 365
Lookup Table Audit Logs 366
Exclude List Audit Logs 366
Audit Logs for Dashboard updates 367

Chapter 9: Data Onboarding and Log Source Management 368
Onboarding your data 368
Security Analytics Best Practices 371
Limit Cloud Link file size 372
Supported Log Sources (Limited Availability) 373
1Password 382
AWS S3 384
Absolute 389
Ad Password Interceptor 392
Aisera 397
Akamai SIEM 402
Algosec 407
AppOmni 412
AppViewX 417
Aruba Clearpass 422

Aruba Networks 427
AVI Networks 432
AWS Autoscaling 437
AWS CloudTrail 442
AWS CloudWatch 447
AWS Config Notification 452
AWS EC2 457
AWS GuardDuty 462
AWS Health 467
AWS SSM 472
AWS VPC DNS 477
AWS VPC Flow 482
AWS WAF 487
Microsoft Azure Active Directory 491
Microsoft Azure Sentinel 500
Bomgar 505
Carbon Black 510
Catalina 515
Cisco ACS 520
Cisco ASA 525
Cisco ESA 530
Cisco ESA Amp 535
Cisco ESA AntiSpam 540
Cisco ESA Antivirus 545
Cisco ESA Authentication 550
Cisco ESA Bounce 555
Cisco ESA CLI Audit 560
Cisco ESA Greymail 565
Cisco ESA HTTP 570
Cisco ESA LDAP 575
Cisco ESA NTP 580
Cisco ESA Quarantine GUI 585
Cisco ESA Reporting 590
Cisco ESA Scanning 595
Cisco ESA Textmail 600
Cisco FTD 605
Cisco Ironport 610
Cisco ISE 615
Cisco Meraki 620
Step 1: Create API key 620

Step 2: Add Cisco Meraki as new log source 620
Step 3: Configure permissions 621
Step 4: Check log source status 622
Step 5: Receive confirmation email 622
Step 1: Ship data to S3 using NXLog 622
Step 2: Set up SQS queue 623
Step 3: Enable AWS S3 notifications 623
Step 4: Add Cisco Meraki as new log source 623
Step 5: Configure permissions 625
Step 6: Check log source status 625
Cloudflare WAF 627
CrowdStrike Event Streams 632
CrowdStrike FDR 637
Cyberark EPV 642
Microsoft Defender 647
Step 1: Ship data to S3 using NXLog 649
Step 2: Set up SQS queue 649
Step 3: Enable AWS S3 notifications 649
Step 4: Add Defender as new log source 650
Step 5: Configure permissions 652
Step 6: Check log source status 652
Microsoft Defender ATP 654
Step 1: Ship data to S3 using NXLog 657
Step 2: Set up SQS queue 657
Step 3: Enable AWS S3 notifications 657
Step 4: Add Defender ATP as new log source 658
Step 5: Configure permissions 660
Step 6: Check log source status 660
Duo 662
ESXi 667
F5 BIG-IP 672
F5 BIG-IP TCL Error 677
Forcepoint 682
Fortinet 687
Google Cloud Platform 692
Step 1: Ship data to S3 using NXLog 700
Step 2: Set up SQS queue 700
Step 3: Enable AWS S3 notifications 700
Step 4: Add GCP VPC or Firewall or Auto as new log source 701
Step 5: Configure permissions 703

Step 6: Check log source status 703
Google SecOps 704
Prerequisites 704
Step 1: Download Google SecOps Service Account Credentials 705
Step 2: Retrieve Google SecOps Identifiers 705
Step 3: Add Google SecOps as new log source 705
Step 4: Configure permissions 707
Step 5: Check log source status 707
Step 6: Receive confirmation email 708
Google Workspace 709
Prerequisites 709
Step 1: Create Google Cloud Project 709
Step 2: Create service account 709
Step 3: Enable Workspace Admin SDK API 709
Step 4: Create API credentials 710
Step 5: Delegate domain-wide authority 710
Step 6: Create new role for new or existing user 711
Step 7: Add Google Workspace as new log source 711
Step 8: Configure permissions 712
Step 9: Check log source status 713
Step 1: Ship data to S3 using NXLog 713
Step 2: Set up SQS queue 713
Step 3: Enable AWS S3 notifications 714
Step 4: Add Google Workspace as new log source 714
Step 5: Configure permissions 716
Step 6: Check log source status 716
GitHub Cloud 718
Guardicore Centra 723
HA Proxy 728
IdentityIQ 733
IIS 738
Infoblox 743
Infoblox Audit 748
Infoblox File 753
JumpCloud 758
Juniper Corero 763
Juniper JUNOS 768
Juniper Switches 773
Linux Audit 778
Linux Auth 783

Mimecast 788
Prerequisites 788
Step 1: Create custom API App 788
Step 2: Add Mimecast as new log source 788
Step 3: Configure permissions 790
Step 4: Check log source status 790
Step 1: Ship data to S3 using NXLog 791
Step 2: Set up SQS queue 791
Step 3: Enable AWS S3 notifications 791
Step 4: Add Mimecast as new log source 792
Step 5: Configure permissions 794
Step 6: Check log source status 794
Mimecast 1.0 795
Prerequisites 795
Step 1: Retrieve custom App ID and App Key 795
Step 2: Create new user 795
Step 3: Add user to admin role 796
Step 4: Create new user group 796
Step 5: Create new authentication profile 796
Step 6: Create new app setting 797
Step 7: Create Access and Secret Keys 797
Step 8: Add Mimecast as new log source 798
Step 9: Configure permissions 799
Step 10: Check log source status 800
Step 1: Ship data to S3 using NXLog 800
Step 2: Set up SQS queue 800
Step 3: Enable AWS S3 notifications 801
Step 4: Add Mimecast as new log source 801
Step 5: Configure permissions 803
Step 6: Check log source status 803
Microsoft DHCP 805
Microsoft Graph Security Alert 810
Miro Audit 815
Microsoft Cluster Services Audit 820
Microsoft Cluster Services Azure 825
Nametag 830
Nasuni Log 835
Nasuni Storage 840
Netskope 845
Step 1: Create API token 845

Step 2: Add Netskope as a new log source 845
Step 3: Configure permissions 847
Step 4: Check log source status 847
Step 1: Ship data to S3 using NXLog 848
Step 2: Set up SQS queue 848
Step 3: Enable AWS S3 notifications 848
Step 4: Add Netskope as new log source 849
Step 5: Configure permissions 851
Step 6: Check log source status 851
NSG Flow 853
Prerequisites 853
Step 1: Register Insights Provider 853
Step 2: Azure storage account 853
Step 3: Obtain Account Access Key 853
Step 4: Add NSG Flow as new log source 853
Step 5: Configure permissions 855
Step 6: Check log source status 855
Step 7: Receive confirmation email 856
NXLog Agent 857
Microsoft Office 365 862
Prerequisites 862
Step 1: Register an App with Azure AD 862
Step 2: Add Office 365 as new log source 863
Step 3: Configure permissions 864
Step 4: Check log source status 865
Step 5: Receive confirmation email 865
Step 1: Ship data to S3 using NXLog 865
Step 2: Set up SQS queue 865
Step 3: Enable AWS S3 notifications 866
Step 4: Add Office365 as new log source 866
Step 5: Configure permissions 868
Step 6: Check log source status 868
Microsoft Office365 Graph 870
Okta 875
Step 1: Create API token 875
Step 2: Add Okta as a new log source 875
Step 3: Configure permissions 876
Step 4: Check log source status 877
Step 1: Ship data to S3 using NXLog 877
Step 2: Set up SQS queue 878

Step 3: Enable AWS S3 notifications 878
Step 4: Add Okta as new log source 878
Step 5: Configure permissions 880
Step 6: Check log source status 880
Okta Agent 882
Okta Radius 887
Okta Radius Access 892
Oracle IAM Access 897
Oracle IAM Errors 902
Oracle IAM Replication 907
Palo Alto Networks Firewall 912
Proofpoint 917
Step 1: Create API token and Service Principal 917
Step 2: Add Proofpoint as new log source 917
Step 3: Configure permissions 918
Step 4: Check log source status 919
Step 5: Receive confirmation email 919
PagerDuty 920
Step 1: Create API token 920
Step 2: Add PagerDuty as a new log source 920
Step 3: Configure permissions 922
Step 4: Check log source status 922
Step 5: Receive confirmation email 923
IBM QRadar 924
Step 1: Create token 924
Step 2: Add QRadar as new log source 924
Step 3: Configure permissions 925
Step 4: Check log source status 926
Step 5: Receive confirmation email 926
PRTG 927
Step 3: Configure permissions 928
Step 4: Check log source status 929
Step 1: Ship data to S3 using NXLog 929
Step 2: Set up SQS queue 929
Step 3: Enable AWS S3 notifications 929
Step 4: Add PRTG as new log source 930
Step 5: Configure permissions 932
Step 6: Check log source status 932
Secure Relay 934
ServiceNow 939

Step 1: Create authentication credentials on ServiceNow 939
Step 2: Add ServiceNow as new log source on Anomali 939
Step 3: Configure permissions 941
Step 4: Check log source status 941
Step 5: Receive confirmation email 942
Step 1: Ship data to S3 using NXLog 942
Step 2: Set up SQS queue 942
Step 3: Enable AWS S3 notifications 942
Step 4: Add ServiceNow as new log source 943
Step 5: Configure permissions 945
Step 6: Check log source status 945
Sumo Logic 947
Step 3: Configure permissions 948
Step 4: Check log source status 949
Step 1: Ship data to S3 using NXLog 949
Step 2: Set up SQS queue 949
Step 3: Enable AWS S3 notifications 949
Step 4: Add Sumo Logic as new log source 950
Step 5: Configure permissions 952
Step 6: Check log source status 952
Suricata 954
Tanium HTTP 959
Thycotic 964
Windows 969
Windows Event 974
Wiz 979
Zscaler DNS 984
Zscaler FW 989
Zscaler NSS Web 994
Zscaler Web 999
Zscaler LSS ZPA App 1004
Zscaler LSS ZPA Auth 1009
Log Transport Services (Limited Availability) 1014
Setting up SQS Queue (Limited Availability) 1015
Using NXLog to Ship Data 1018
Before You Begin 1018
Step 1. Set Up NXLog Enterprise Edition Agent 1018
Step 2. Deploy NXLog Agent 1018
Step 3. Prepare Configuration File 1018

Reference Information 1021
Appendix A: Reserved Field Names and Keywords 1022
Appendix B: Sample Patterns for Dissect, Grok, Regex, and Ruby Parsers 1023
Dissect 1023
Grok 1024
Regex 1024
Ruby 1025
Appendix C: ThreatStream Indicator Types 1028
Appendix D: Anomali Security Analytics Alert Messages 1049
Appendix E: Using the Anomali Security Analytics RESTful API 1069
About the API 1069
Using REST APIs to Upload Asset Information 1071
Using REST APIs to Get DGA Score Information 1073
Using REST APIs to Upload a DGA Exclude List 1074
Using REST API to Run a Search 1076
Using REST API to Run a Forensics and Retrospective Search 1078
Using Alerts (Classic UI) 1083
Alert Rule Types 1083
Alert Filters 1083
Alert Actions 1084
Configure an Event Search Alert 1087
Modify an Alert Configuration 1102
Clone an Alert Configuration 1102
Delete an Alert Configuration 1102
Review Alert Rule Details 1103

Chapter 1: Anomali Security Analytics Overview

Anomali Security Analytics delivers a powerful, integrated cybersecurity solution that empowers organizations to enhance their defenses with advanced features such as log aggregation, a scalable data lake for rapid insight retrieval, and customized analytics dashboards. Security Analytics offers automated multilayer threat detection, behavior analytics, and an interactive investigation workbench, complemented by alert enrichment and automated response capabilities. With tools for detection triage, domain prediction, and proactive threat hunting, Anomali ensures that your enterprise can swiftly identify, analyze, and respond to potential security threats, safeguarding your digital environment against current and future risks.

Anomali Security Analytics Key Objectives

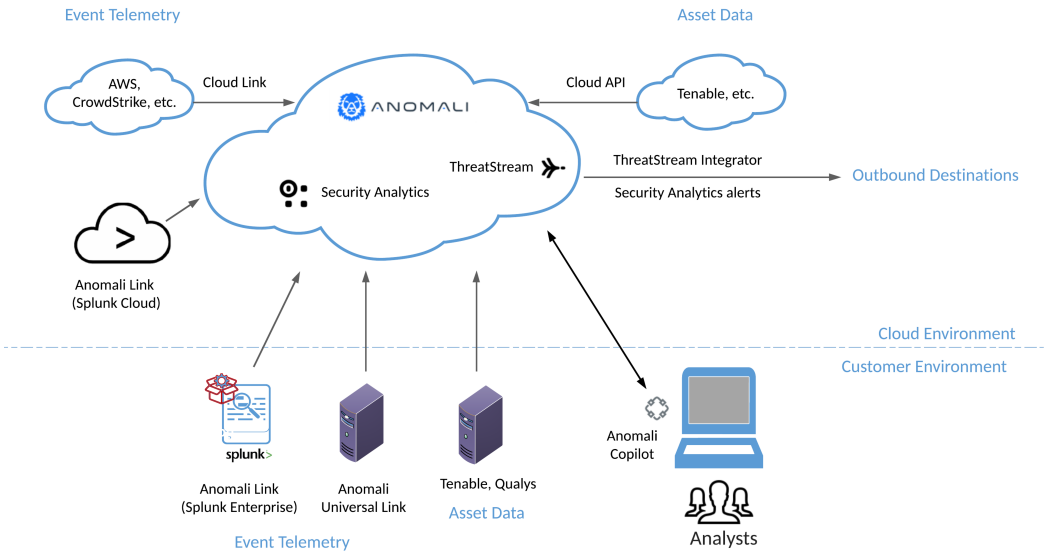
With an easy-to-use, web-based interface that provides interactive dashboards and predefined reports, the Anomali Security Analytics platform enables your security team to:

- Gain visibility over events matching indicators of compromise (IOCs)
- Gain visibility over events matching connections to Domain Generated Algorithm (DGA) domains
- Perform retrospective searches for advanced forensics
- Generate alerts based on criteria that you specify

By filtering out the noise, correlating event data from your network, and analyzing this data to identify real threats, Anomali Security Analytics helps your security team prioritize, focus, and optimize threat response efforts.

Anomali Security Analytics Deployment Components

The following illustration shows a basic Security Analytics deployment. Security Analytics ingests event telemetry and asset data from your organization's cloud sources and on-premise sources. Security Analytics correlates events with ThreatStream intelligence and enriches the matching results with asset details. Optionally, you can configure Security Analytics alert actions to send outbound messages or add tags to ThreatStream IOCs and use ThreatStream Integrator to update outbound destinations.



The following sections describe the basic components in detail.

Anomali Security Analytics

The Anomali Security Analytics system has the following specialized components:

- Web-based user interface
- Network security event telemetry collection
- Security intelligence and asset details correlation
- Forensic service
- Alert service

Threat Intelligence

Anomali Security Analytics correlates event logs with intelligence your organization maintains in Anomali ThreatStream. ThreatStream is a Threat Intelligence Platform (TIP) that aggregates threat intelligence from diverse sources, provides an integrated set of tools for fast and efficient investigations, and delivers operationalized threat intelligence to your security controls at machine speed.

Security Analytics serves information about detected observables (sometimes referred to as *sightings*) to the ThreatStream observable details pages and the My Attacks report. In cloud deployments, you do not need to do anything to enable this integration.

Refer to ThreatStream online help for complete details.

Anomali Link Software

You deploy one or more Anomali Link software instances. Link software is deployed on the SIEM system or on another system in your environment—sources on premises in your local network. A Link instance connects to Security Analytics on one side and to a SIEM (or other event source) on the other side. Links perform the following work:

- Collect data from the event source
- Parse the data into normalized event log fields
- Upload the normalized event log data to Security Analytics

Anomali Copilot

Anomali Copilot is a free browser extension for Google Chrome, Microsoft Edge, and Mozilla Firefox from Anomali. Copilot uses natural language processing (NLP) to scan the contents of a web page you are currently viewing. On the web page, Copilot highlights all cyber threat information—actors, malware, and observables. Copilot integrates with Security Analytics in the backend. As you view a web page,

Copilot highlights the indicators that have matched events on your network. You can drill down directly from Copilot to Security Analytics to get more details about the matched events and view the details about the indicator.

You can find Copilot browser extension package files, Office 365 add-in package files, and the *Anomali Copilot User Guide* on ThreatStream Downloads.

Chapter 2: Using Anomali Security Analytics Dashboards

You can use the Security Analytics dashboards to gain insight about the threats observed in your environment, filter out the noise from irrelevant indicators, and drill into details about indicators (and related events) that may be of interest to you.

This chapter includes the following topics:

Getting Started with Dashboards 23
Overview Dashboard 28
Multi Dimensional Dashboard 38
Match Analysis Dashboard 49

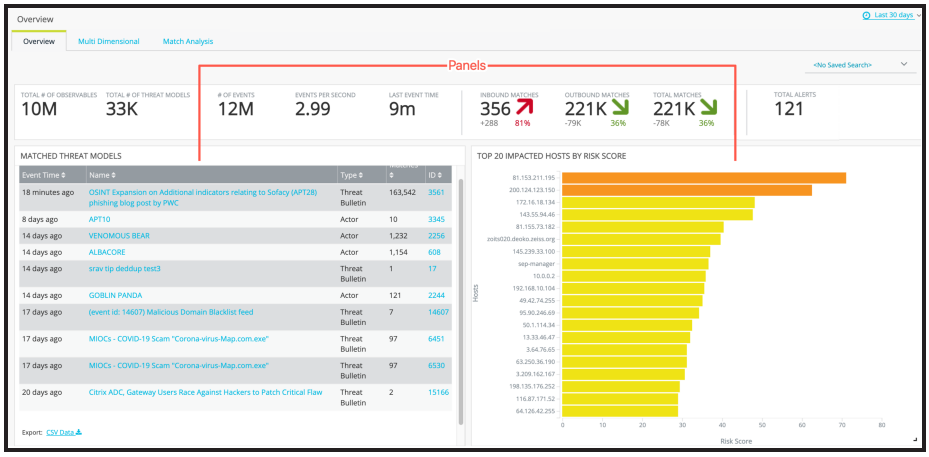
Getting Started with Dashboards

This topic describes common Security Analytics Dashboard features.

> **Note:** Security Analytics Dashboards are separate from AQL Dashboards. For information about AQL Dashboards, go to the Anomali Dashboards Help Center.

Panels

A dashboard comprises panels, which include visualizations or table presentations of Security Analytics statistics.



To resize a panel:

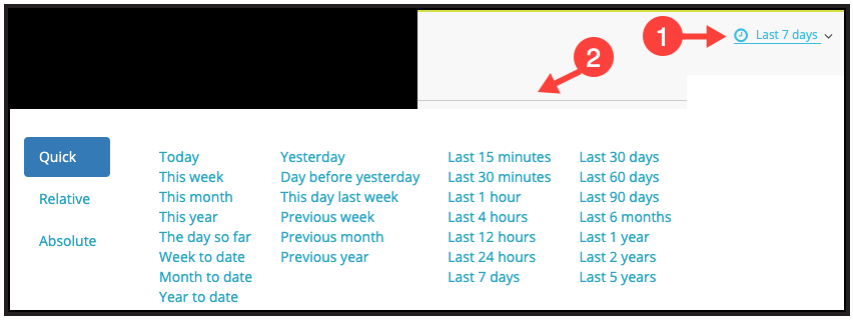
1. Hover over the lower-right corner.
2. When the cursor changes to an arrow, click and drag the panel to the size you prefer.

To rearrange panels:

- Click the title bar and drag the panel to the location on the dashboard you prefer.

Time Period

By default, a dashboard displays statistics for the last 7 days. You can use the time period picker in the top-right corner of the page to select a different time range.



1	Click the current time period filter to display the time period picker.
2	Use the time period picker to select a time period. There are three sets of selectors: • **Quick**—A set of time expressions that are easy to apply by simply clicking your selection. • **Relative**— A set of controls to configure a time range relative to the present time. • **Absolute**—A set of controls to configure a time range between any two points on the calendar.

Notes:

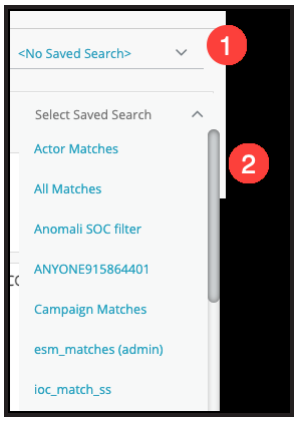
- The time period filter is based on event time; in other words, the timestamp in the event log.
- The event retention policy renders event log data unavailable for search and dashboards after a configured number of days.
- Events received from log ingestion backfill jobs can have dates that go farther back than the retention policy expiration date. For example, a backfill job might ingest logs with event timestamps from up to 5 years ago, and those are the events that are included when the **Last 5 years** filter is applied.

- The default time range is specified in My Profile settings. See "Change the Default Date Range Filter" on page 293.
- If you change the time period, the time period that you specify persists across all Dashboard and Activity search pages until you change it again or log out of your browser session.

Saved Search

By default, dashboards display information based on results of a predefined query.

You can use the Saved Search picker to make the information in the dashboards based on a saved search. This selection affects only the current web session of the currently logged in user.



1	Click the current saved search filter to display the saved search picker.
2	Use the saved search picker to select a new saved search.

See "Managing Saved Searches" on page 254 for information on defining saved search queries.

Export CSV

Export: CSV Data	Panels with table presentations include a link below the tables. Click the **CSV Data** link to download the table as a CSV file. Rename the file if you want, choose a location for the exported file, and then click **Save**.

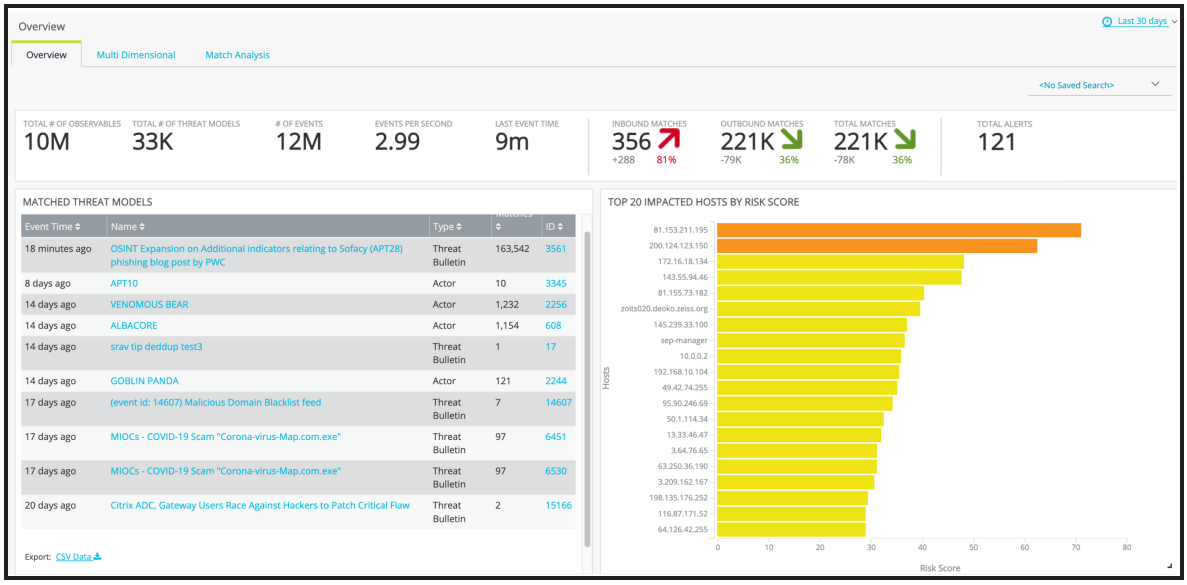
Hypertext Links

The visualizations or table presentations in panels may include hypertext links that allow you to filter data in the current view, drill-down to a detailed view, pivot to related content, or take action.

Overview Dashboard

The Overview Dashboard provides a high-level view of threats in your network. The interactive visualizations of Security Analytics statistics allow you to drill down further on any element of concern for a deeper analysis.

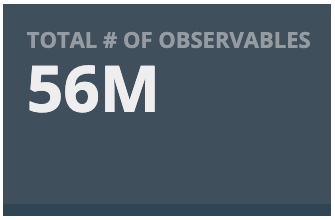
The following figure shows the Overview Dashboard. The sections that follow provide details about the Overview Dashboard panels.



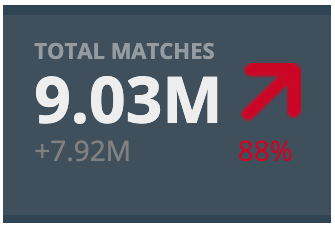
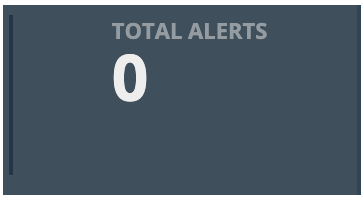
For an overview of dashboard time period and saved search filters, file export, and navigation elements, see "Getting Started with Dashboards" on page 23.

Top Panel

The top panel contains the following counters.

Counter	Description
	**Total # of Observables**—Count of observables (also known as indicators) from threat intelligence sources. Note: This is a cumulative count of the set of observables used for correlation since the initial deployment.

Counter	Description
TOTAL # OF THREAT MODELS 140K	**# of Threat Models**—Count of threat models from threat intelligence sources. Note: This is a cumulative count of the set of threat models used for correlation since the initial deployment.
# OF EVENTS 1.05B	**# of Events**—Count of events received from log sources during the selected time period.
EVENTS PER SECOND 387	**Events per Second**—Event log ingestion rate during the selected time period.
LAST EVENT TIME 2h	**Last Event Time**—Hours since the last event was received.
INBOUND MATCHES 204K +26K 13%	**Inbound Matches**—Count* of inbound events that matched indicators during the selected time period. Inbound events are the ones in which a device on your network is the destination of the event.
OUTBOUND MATCHES 7.74M +6.99M 90%	**Outbound Matches**—Count* of outbound events that matched indicators during the selected time period. Outbound events are the ones in which a device on your network is the source of the event.

Counter	Description
	**Total Matches**—Count* of indicators that have matched your event data during the selected time period. The total includes inbound, outbound, and non-network-related matches, such as file hash and email matches.
	**Total Alerts**—Count* of alert events during the selected time period.

* These counts include three numbers:

- The number in large font is the count of indicator matches in the selected time period. The default time period is **Last 7 days**.
- The number in the smaller font is a comparison in number of indicator matches in the prior time period. If the selected time period for the dashboard is **Last 7 days**, the time period for comparison is the period from 14 days ago to 7 days ago. A plus (+) or minus (-) sign indicates an increase or decrease in the number of matches.
- Trend is the percent increase or decrease based on the two time periods. This change is also shown by the trend arrow.

Matched Threat Models

This panel displays a table showing the 10 most recent threat models that matched events.

MATCHED THREAT MODELS View All Filter

Event Time	Name	Type	Matches	ID
10 hours ago	APT41	Actor	11,911	2250
10 hours ago	APT28	Actor	346	2314
10 hours ago	APT41	Actor	11,892	2710
10 hours ago	APT28	Actor	346	2773
10 hours ago	APT41	Actor	11,827	3108
10 hours ago	APT28	Actor	346	3268
10 hours ago	APT41	Actor	11,819	4969
10 hours ago	SILENT CHOLLIMA	Actor	416	5309
10 hours ago	COMMENT PANDA	Actor	155,879	5313
10 hours ago	MUMMY SPIDER	Actor	50,143	5340

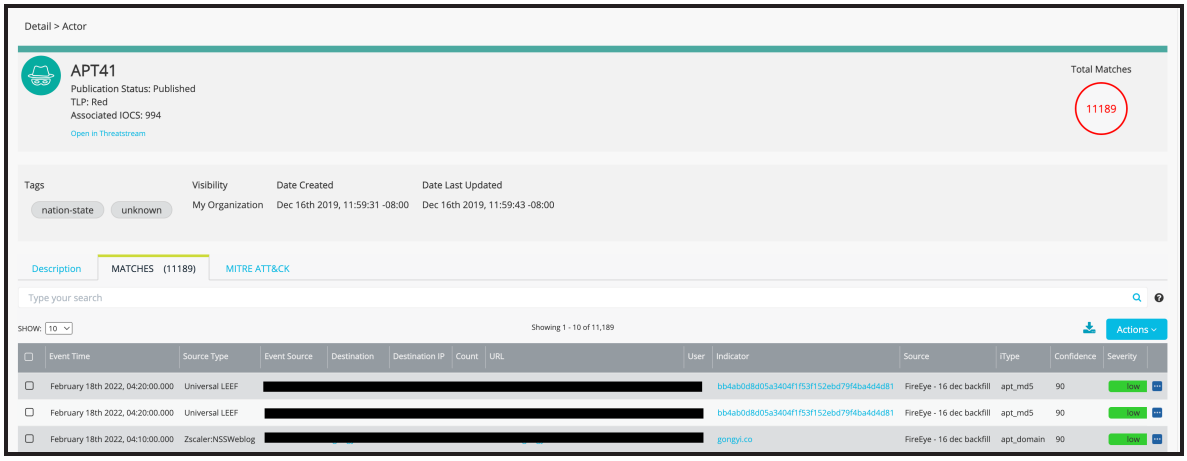
Export: CSV Data

The following table describes the Matched Threat Model table columns.

Column	Description
Event Time	Time relative to the present that the event occurred.
Name	The name of the threat model entity.
Type	Actor, Attack Pattern, Campaign, Threat Bulletin, TTP, Vulnerability. You can use the **Filter** control above the table to display the 10 most recent matches for a selected threat model type.
Matches	Count of unique matches during the selected time period. The default time period is **Last 7 days**. You can use the time period picker in the top-right corner of the page to change the time period.
ID	Threat Model ID in ThreatStream.

Drill-in on Items of Concern

Click the linked threat model name to issue an Activity page search for the selected threat model entity. The following figure shows the search results for a selected Actor.



> **Note:** The Matched Threat Models panel displays the number of *unique* matches, which is an approximate count of unique values (Cardinality Aggregation). When you drilldown from the panel to a threat model details page, the number on the details screen displays the total (not unique) number of matches. As a result, at times, the number of matches on the two screens may differ slightly.

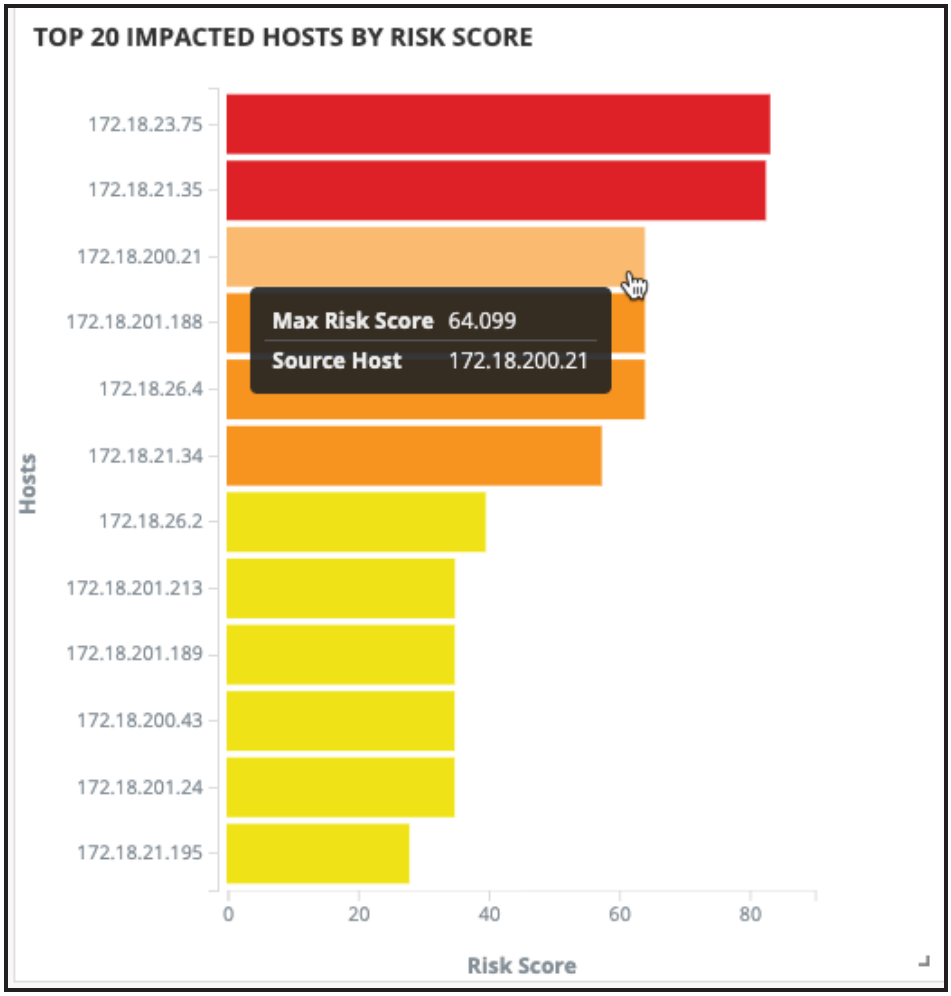
Top 20 Impacted Hosts by Risk Score

This panel displays a bar chart showing the top 20 hosts with events that matched indicators, ordered by risk score. Risk score statistics are re-calculated each day, and the data for the day is used to update the panel between midnight and 03:00 AM. Updates are based on events occurring in the previous 1 day. Events ingested via backfill jobs may have event times earlier than the previous 1 day. These backfill events do not impact risk score.

Risk score is a weighted score based on multiple factors, including indicator confidence, severity, indicator type, and the number of sources reporting the indicator. Event logs where the action reported is equivalent to "blocked" do no impact risk score.

Gain Insight Quickly

Hover over the bars to display the score for an individual event source. Click a bar to display the Asset Details page for the host.

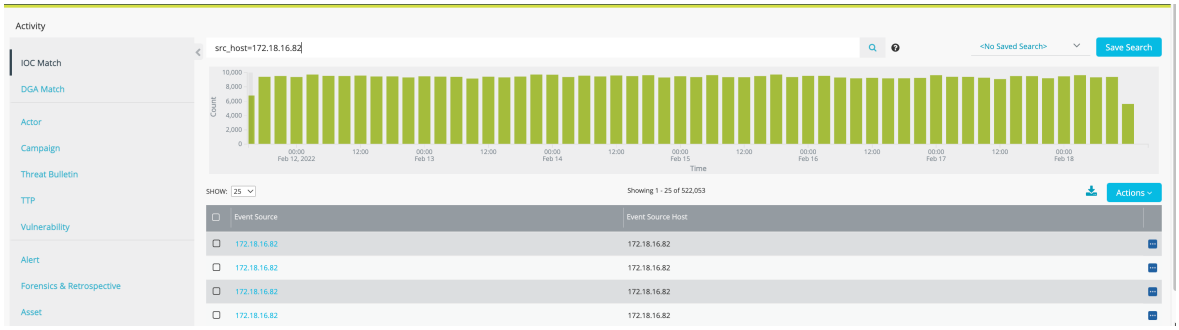


The following table describes the bar chart.

Field	Description
Max Risk Score	The highest risk score reported during the selected time period. Risk score is a weighted score based on multiple factors, including indicator confidence, severity, indicator type, number of sources reporting the indicator, asset criticality, and directionality of the match.
Event Source	Host IP address.

Drill-In on Items of Concern

Click a bar in the chart to issue an IOC Match activity search for the particular host.

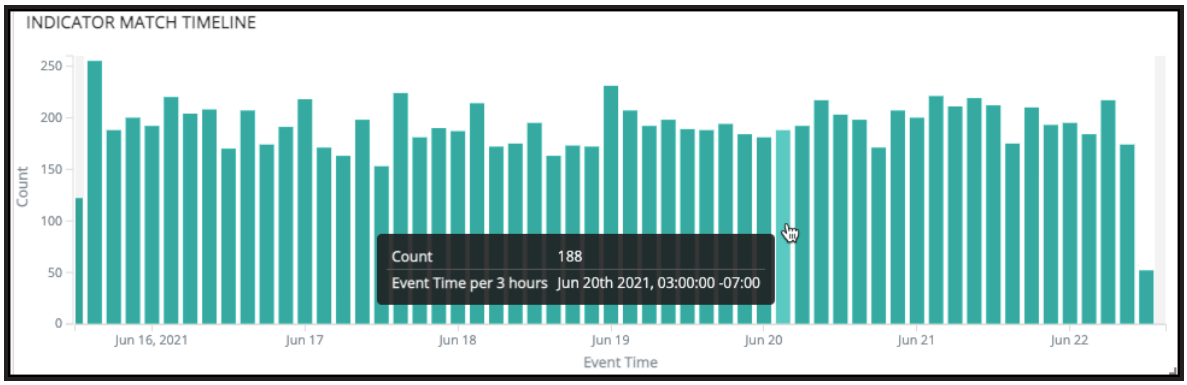


Indicator Match Timeline

This panel displays a bar chart showing the trend in matches over time.

Gain Insight Quickly

Hover over the bars to display the count for a time period.



The following table describes the graph.

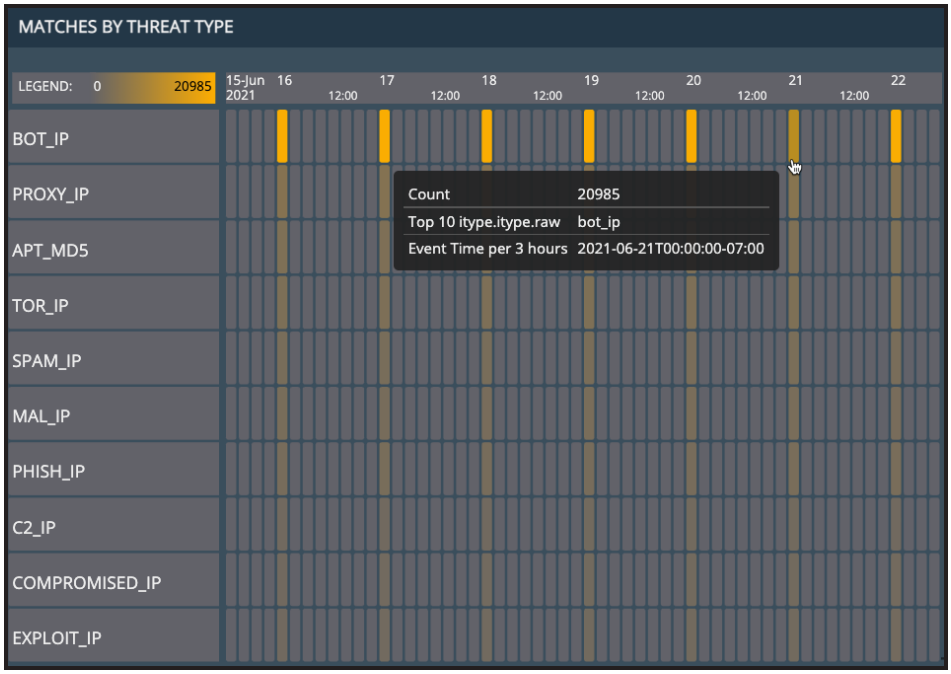
Field	Description
Count	Total indicator matches for the time period.
Event Time	The granularity of the time axis is based on the dashboard time period selection. The default time period is **Last 7 days**. In a chart with this granularity, a bar indicates the count in a 3 hour period.

Drill-in on Items of Concern

Click a bar in the chart to issue an IOC Match search. The following figure shows the Activity page search results for events with the selected time period.

Matches by Threat Type

This panel displays a time-volume meter for the top matched threat types.



The following table describes the statistics.

Dimension	Description
Count	Total indicator matches for the time period. The volume indicator ranges from dim to bright. The greater the count, the brighter the volume.
Threat Type	Indicator type. See "ThreatStream Indicator Types" on page 1028 for a complete reference.
Time	The granularity of the time axis is based on the dashboard time period selection. The default time period is **Last 7 days**. In a chart with this granularity, each bar indicates the count in a 3 hour period.

Drill-in on Items of Concern

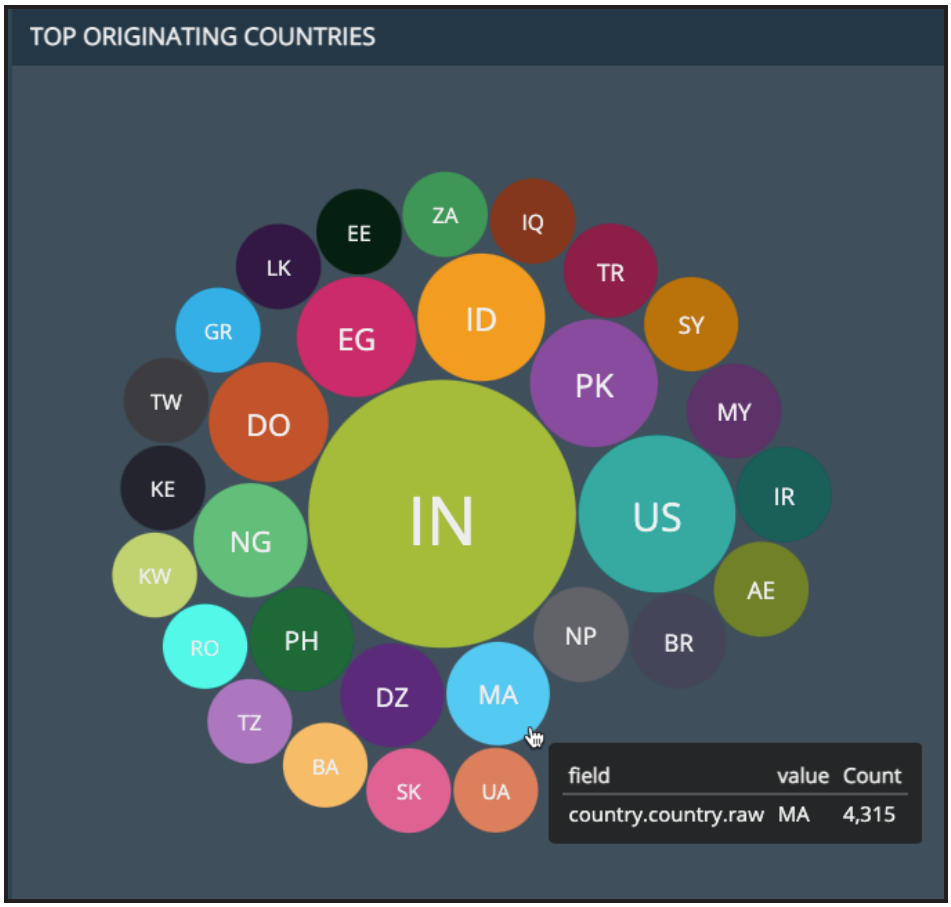
Click a cell in the chart to issue an IOC Match search. The following figure shows the Activity page search results for events with the selected impact type.

Top Originating Countries

This panel displays a bubble chart of the indicator matches by country. The larger the bubble, the higher the score.

Gain Insight Quickly

Hover over a bubble to display the indicator value and score.

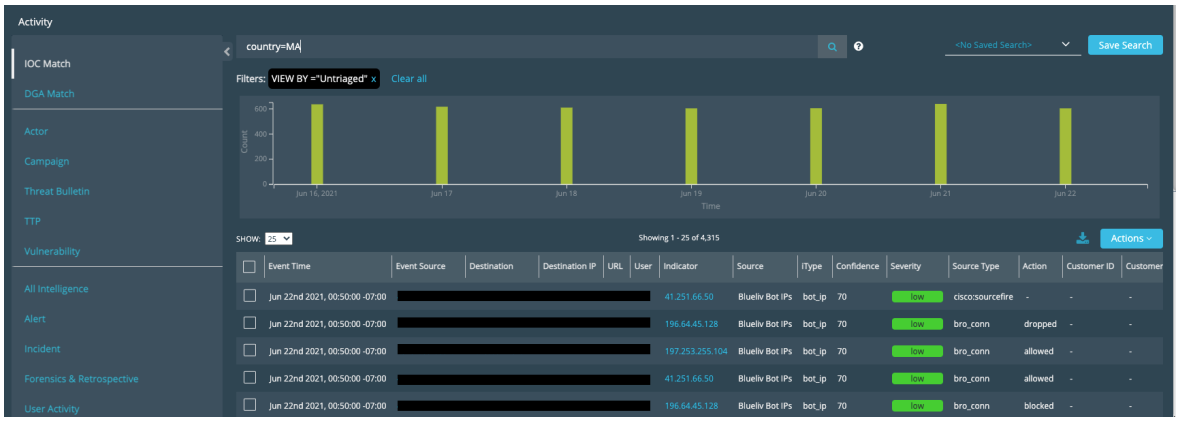


The following table describes the chart.

Field	Description
field-value	The field-value pair used for this visualization is country.country.raw - <country>.
Count	Matches where the specified country was the source of the tracked event.

Drill-In on Items of Concern

Click the country code in a bubble to issue an IOC Match search on the Activity page, filtered for the selected country. The following figure shows IOC Match search results for Morocco.

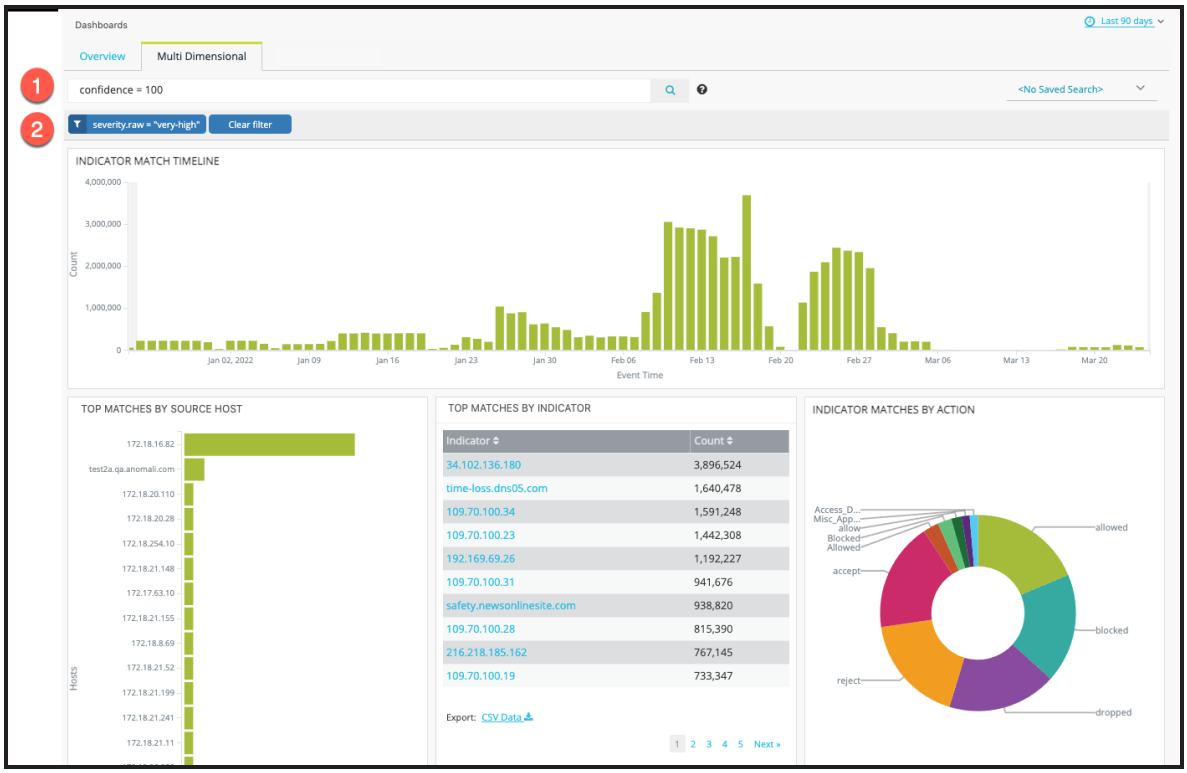


Multi Dimensional Dashboard

The Multi Dimensional Dashboard has ten visualizations and table panels that show the occurrences of IOC matches over time. The panels bring different elements of IOC matching into focus—for example, IOC matches over time or IOC matches by source. You can use the search box to form a filter expression, and you can also apply additional filters by clicking data points in the panels.

When a filter is applied or cleared, Security Analytics updates all of the Multi Dimensional Dashboard panels to reflect the new results.

The following figure shows the Multi Dimensional Dashboard. The sections that follow provide details about the Multi Dimensional Dashboard panels.

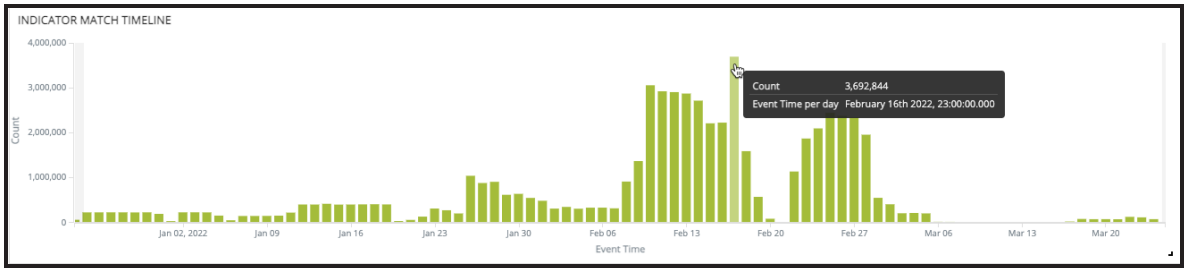


1	Query search box. See "Getting Started with Activity Search" on page 57.
2	Data point filters. To remove a single filter, hover over it to reveal an **X** you can click to remove it. To clear all data point filters, click **Clear filter**.

For an overview of dashboard time period and saved search filters, file export, and navigation elements, see "Getting Started with Dashboards" on page 23.

Indicator Match Timeline

This panel displays a bar graph showing the count of indicator matches over time. Click a bar to filter by date. Click and drag overa range of bars to set a date range filter. The filter is applied to all panels in the dashboard.

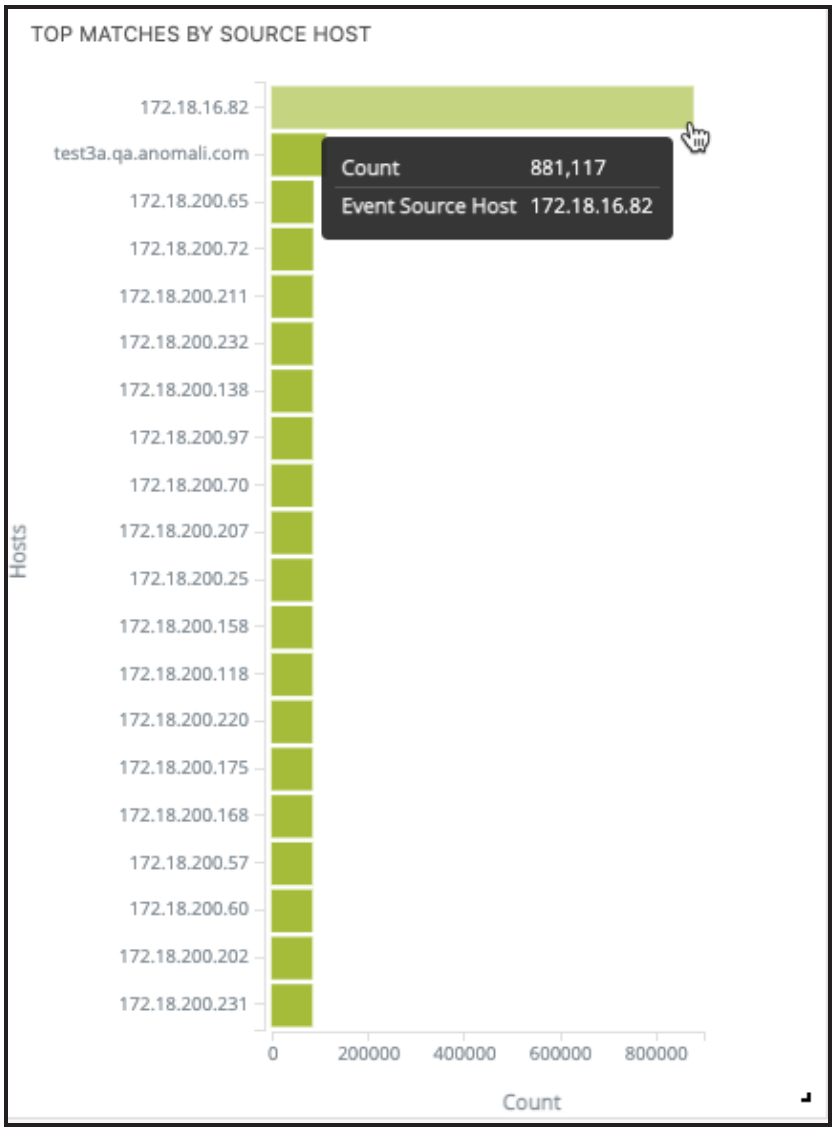


The following table describes the graph.

Field	Description
Count	Total indicator matches for the time period.
Event Time	The granularity of the time axis is based on the dashboard time period selection. **Note**: The default time period is **Last 7 days**. In a chart with this granularity, a bar indicates the count in a 3 hour period. You can change the default time period associated with your user profile. See "Modifying My Profile" on page 293.

Top Matches By Source Host

This panel displays a bar chart showing the top 20 match counts by source host during the selected time period. Hover over the bars to display the match count. Click a bar to apply a data point filter to the Multi Dimensional Dashboard.



The following table describes the bar chart.

Field	Description
Count	Count of event matches during the selected time period.
Event Source Host	An event source host value derived from asset_src_hostname, event.src, or event_ip fields, in that order. The hostname provided by the asset enrichment would be most readable, so if it data exists for it, it is used. If not, then the other source fields are evaluated.

Top 10 Destination Ports

This panel displays a table listing the top 10 destination ports in matched events. Click a destination port to apply a data point filter to the Multi Dimensional Dashboard.

TOP 10 DESTINATION PORTS

Destination Port	Count
0	530,106
80	213,978
1025	447
490	298
511	149
443	108
3305	106
833	18
42423	17
1701	6

Export: CSV Data

The following table describes the Top 10 Destination Ports table columns.

Column	Description
Destination Port	The destination port in the matching event log.
Count	Count of events with this destination port in matched events during the selected time period.

Top Matches By Indicator

This panel displays a table listing the top 50 match counts by indicator during the selected time period. Click an indicator value to apply a data point filter to the Multi Dimensional Dashboard.

TOP MATCHES BY INDICATOR

Indicator	Count
34.102.136.180	3,896,524
time-loss.dns05.com	1,640,478
109.70.100.34	1,591,248
109.70.100.23	1,442,308
192.169.69.26	1,192,227
109.70.100.31	941,676
safety.newsonlinesite.com	938,820
109.70.100.28	815,390
216.218.185.162	767,145
109.70.100.19	733,347

Export: CSV Data

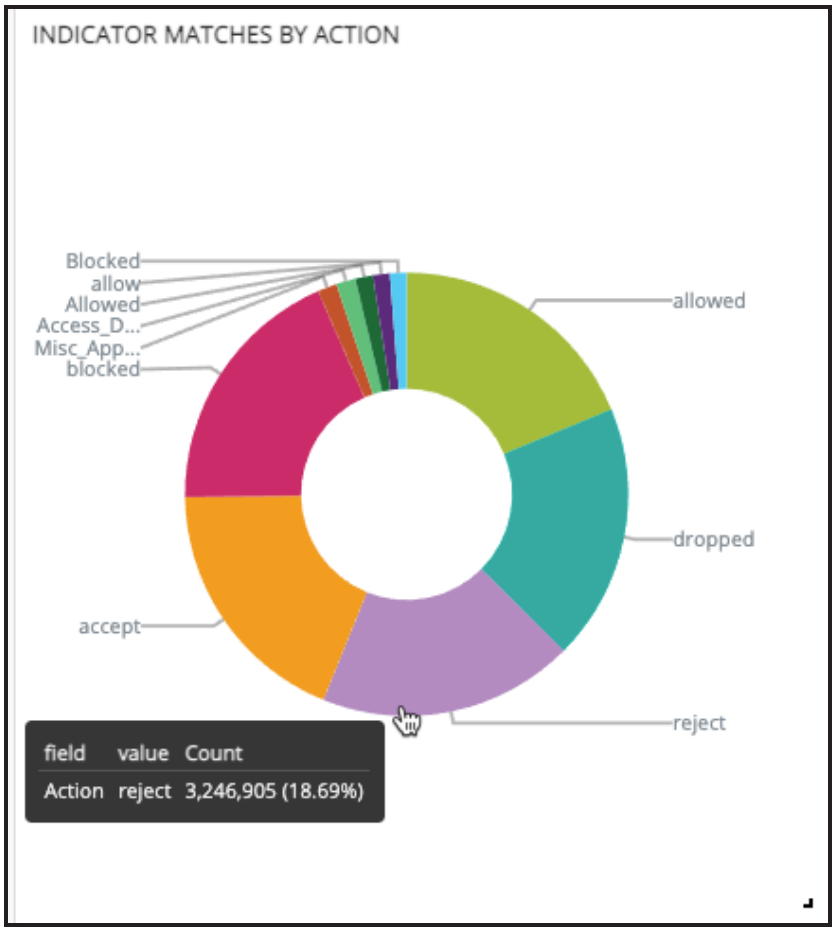
1 2 3 4 5 Next »

The following table describes the To Matches By Indicators table columns.

Column	Description
Indicator	The matching indicator value.
Count	Count of events with this value in matched event logs during the selected time period.

Indicator Matches by Action

This panel displays a doughnut chart showing the distribution of actions identified in event logs for matches. Hover over a band in the doughnut to display the count for an individual action. Click a band to apply a data point filter to the Multi Dimensional Dashboard.

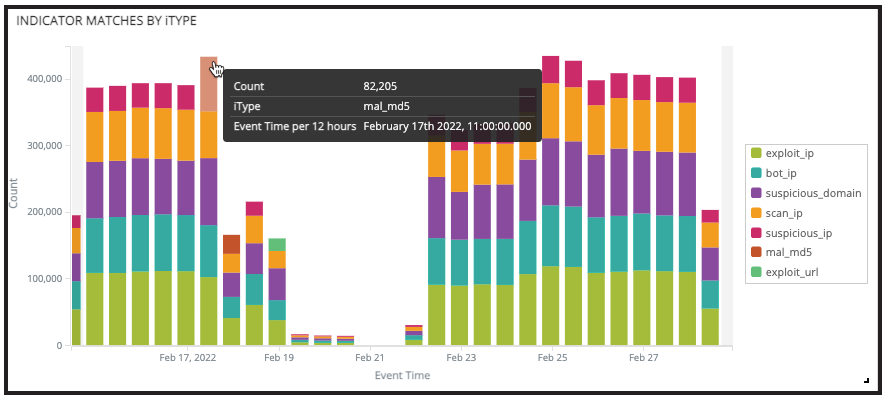


The following table describes the statistics.

Column	Description
field-value	Action: allowed, dropped, blocked, unknown.
Count	Count of events with this action in matched event logs during the selected time period.

Indicator Matches by iType

This panel displays a bar chart showing the distribution of iTypes in matched event logs during the selected time period. Hover over a band in the bar to display the count for an individual iType. Click a band in the bar to apply a data point filter to the Multi Dimensional Dashboard. Click and drag over a range of bars to change the time range filter.

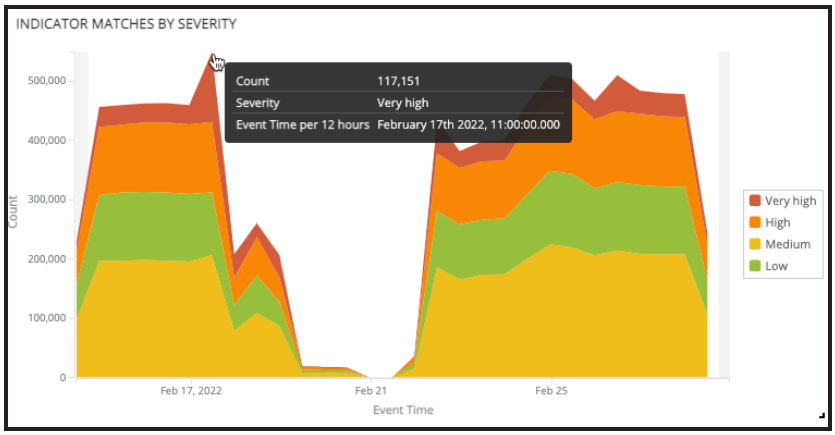


The following table describes the statistics.

Column	Description
Count	Count of events with this iType in matched event logs during the selected time period.
iType	Indicator type. See "ThreatStream Indicator Types" on page 1028 for a complete reference.
Event Time	The granularity of the time axis is based on the dashboard time period selection. **Note**: The default time period is **Last 7 days**. In a chart with this granularity, a bar indicates the count in a 3 hour period. You can change the default time period associated with your user profile. See "Modifying My Profile" on page 293.

Indicator Matches by Severity

This panel displays an area chart showing the distribution of severity in matched event logs during the selected time period. Hover over a band in the area to display the count for an individual severity. Click a band to apply a data point filter to the Multi Dimensional Dashboard. Click and drag over a range of dates to change the time range filter.

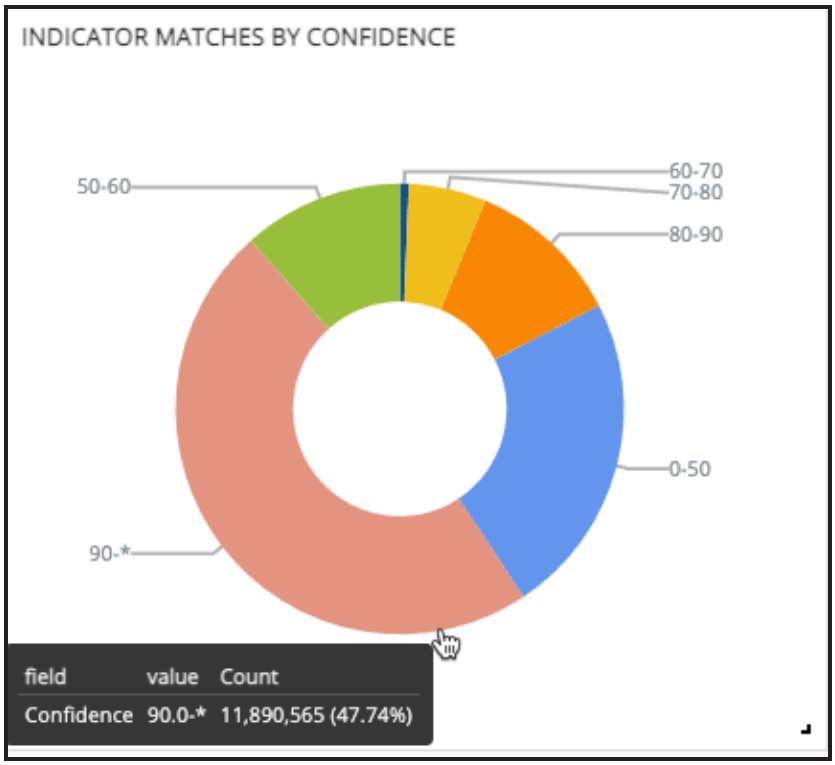


The following table describes the statistics.

Column	Description
Count	Count of events with this severity in matched event logs during the selected time period.
Severity	Very-High, High, Medium, Low.
Event Time	The granularity of the time axis is based on the dashboard time period selection.

Indicator Matches by Confidence

This panel displays a doughnut chart showing the distribution of confidence scores in matched event logs during the selected time period. Hover over a band in the doughnut to display the count for an individual confidence score. Click a band to apply a data point filter to the Multi Dimensional Dashboard.



The following table describes the statistics.

Column	Description
field-value	Confidence score with the specified value.
Count	Count of events with this confidence score in matched event logs during the selected time period.

Indicator Matches by Geo Location

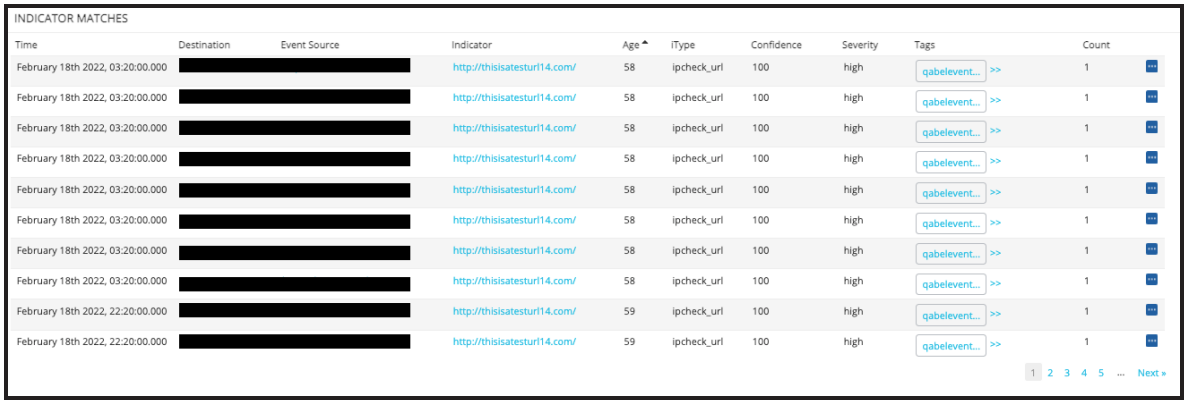
This panel displays an area chart showing the extent of indicator matches in global locations during the selected time period. Hover over the volume circle to display data point statistics. You cannot filter the Multi Dimensional Dashboard through interactions with this panel.

The following table describes the statistics.

Column	Description
Count	Count of events with this action in matched event logs during the selected time period.
Center	Latitude and Longitude for the location.

Indicator Matches

This panel displays an IOC Match table. You cannot filter the Multi Dimensional Dashboard through interactions with this panel.



The following table describes the Indicator Matches table columns.

Column	Description
Time	Event timestamp.
Destination	Destination IP address in event log.

Column	Description
Event Source	Source IP address in event log.
Indicator	Matching indicator value. You can click the value to display a context menu that allows you to perform a retrospective search for the indicator value.
Age	How long ago was the indicator first downloaded on Security Analytics.
iType	Indicator type. See "ThreatStream Indicator Types" on page 1028 for a complete reference.
Confidence	Score from 0 to 100, as reported by the threat feed provider.
Severity	Very-High, High, Medium, Low.
Tags	Any user-defined tags associated with the indicator.
Count	Number of matches per this event log.
	Click the Details icon to view more details about an event.

Match Analysis Dashboard

The Match Analysis Dashboard provides analytics about the threat intelligence feeds, indicator types, indicators, and DGA domains that match events in your network. These analytics can be useful in determining the effectiveness or noise-level of a threat intelligence element. If a premium feed shows matches on events, you can be certain that the premium feed is valuable to your business and its security operations. Likewise, if particular feeds or indicator types are unnecessary, you can create filters to suppress them, or you might unsubscribe.

The following figure shows the Match Analysis Dashboard. The sections that follow provide details about the Match Analysis Dashboard panels.

For an overview of dashboard time period and saved search filters, file export, and navigation elements, see "Getting Started with Dashboards" on page 23.

Note:

- Statistics on the Match Analysis dashboard are not real-time statistics. The statistics are based on daily counts. The counts are recorded daily at a time randomly selected for the customer, and that is the time that the count for the previous calendar day is recorded. Therefore, if you select time filters that are more granular than one day, such as **Last 1 hour** or **Last 4 hours**, the Match Analysis panels will indicate "No results found."

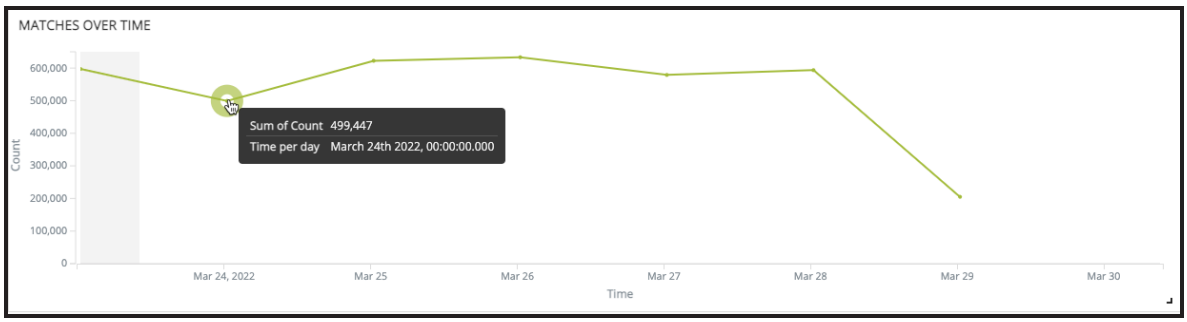
- When you select a time period longer than a day, be aware that the counts do not include events from the current day. For example, the default time period is **Last 7 days**, which means "the last 7 days for which data was recorded." If your enterprise encountered an attack beginning at 08:00, you will not yet see the spike in indicator or victim counts on the Match Analysis dashboard. To see events from the current day, Anomali recommends that you perform a search from the Activity page, which provides a granular view of the recent activity up to the current time. See "Getting Started with Activity Search" on page 57 for complete details.

- In addition, note that the counts reported for Distinct Indicators and Victims are the statistical max values for any day during the reporting period. For example, when the **Last 7 days** time period is selected, the Distinct Indicators count reported is the

highest daily count of distinct indicators for the previous 7 days for which data was recorded. If the daily counts were 1, 4, 1, 2, 2, 1, and 1, the Distinct Indicators count would be 4.

Matches Over Time

This panel displays a line graph of the total indicator match count over time.



The following table describes the chart.

Element	Description
Count	Running total count of matches. The running total is recorded once per day.
Time	The granularity of the time axis is based on the dashboard time period selection. The default time period is **Last 7 days**. You can change the default time period associated with your user profile. See "Modifying My Profile" on page 293.

Matches by Feed

This panel displays a table summarizing matches by threat intelligence feed.

MATCHES BY FEED

Feed	Feed Name	Count	Distinct Indicators	Victims
721	MISP CIRCL - copy for richard	57,203	364	42
743	MISP CIRCL - copy for richard	57,203	364	42
513	CrowdStrike Falcon X final test3	55,915	546	417
22	MISP Doc	47,900	834	250
0	Analyst	35,084	538	250
510	CrowdStrike Falcon X final test2	39,510	372	238
296	CrowdStrike Falcon X test	39,472	366	196
723	MISP CIRCL - copy for robert	30,645	229	42
73	FireEye - fd-4850	23,001	178	111
60	FireEye - Gulshan	18,360	149	58

Export: CSV Data

1 2 3 4 5 ... Next »

The following table describes the Matches by Feed table columns.

Column	Description
Feed	The Anomali Security Analytics ID assigned to the feed. Values in this column are hyperlinks: • Right-click a feed ID value and select **Suppress this feed** to exclude it from future matches. You can review the list of suppressed feeds on the Mange > Exclude List page. See "Manage the Suppressed Feeds List" on page 281. • Click a feed ID value to filter all panels on the Match Analysis Dashboard by the selected feed ID. When you filter by feed ID, the Match Analysis Dashboard displays the filter expression above the panels, as well as a **Clear Filter** button that allows you to clear it.
Feed Name	The name of the threat intelligence feed.
Count	Total event matches for this feed during the selected time period.

Column	Description
Distinct Indicators	The highest daily count of distinct matches to indicators in this feed during the selected time period.
Victims	The highest daily count of systems or hosts that were impacted by the indicators in this feed during the selected time period.

Matches by iType

This panel displays a table summarizing matches by iType. See "ThreatStream Indicator Types" on page 1028 for a list of indicator types and their descriptions.

MATCHES BY ITYPE

Value	Count	Distinct Indicators
apt_ip	632,640	146
apt_domain	621,024	860
phish_ip	444,855	90
exploit_ip	386,443	26
suspicious_domain	294,343	199
bot_ip	248,960	16
scan_ip	248,475	12
mal_md5	167,669	1,559
mal_ip	142,427	90
suspicious_ip	134,644	5

Export: CSV Data

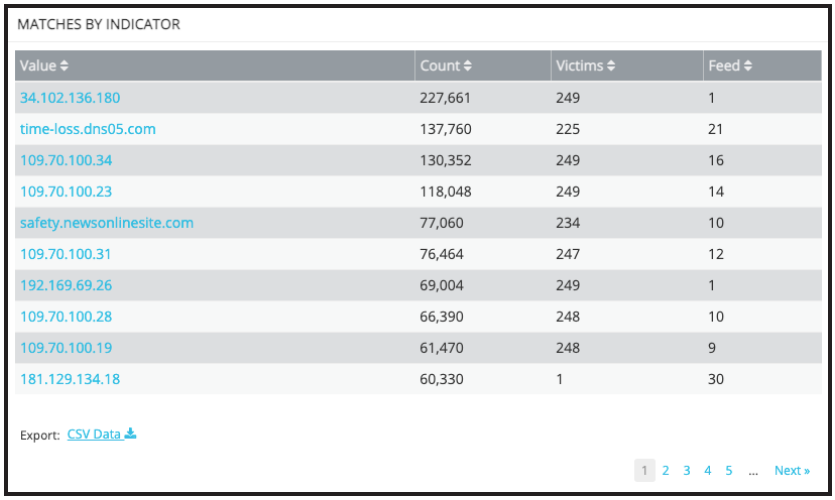
1 2 3 Next »

The following table describes the Matches by iType table columns.

Column	Description
Value	iType short name. Values in this column are hyperlinks. • Right-click an iType value and select **Suppress this iType** to exclude it from future matches. You can review the list of suppressed iTypes on the Mange > Exclude List page. See "Manage the Suppressed iTypes List" on page 279. • Click an iType value to issue an IOC Match search on the Activity page, filtered for the selected iType value.
Count	Total event matches for this iType during the selected time period.
Distinct Indicators	The highest daily distinct count of indicators with this iType value during the selected time period. A *distinct count* returns the number of different indicators having this iType value.

Matches by Indicator

This panel displays a table summarizing matches by Indicator.



MATCHES BY INDICATOR

Value	Count	Victims	Feed
34.102.136.180	227,661	249	1
time-loss.dns05.com	137,760	225	21
109.70.100.34	130,352	249	16
109.70.100.23	118,048	249	14
safety.newsonlinesite.com	77,060	234	10
109.70.100.31	76,464	247	12
192.169.69.26	69,004	249	1
109.70.100.28	66,390	248	10
109.70.100.19	61,470	248	9
181.129.134.18	60,330	1	30

Export: CSV Data

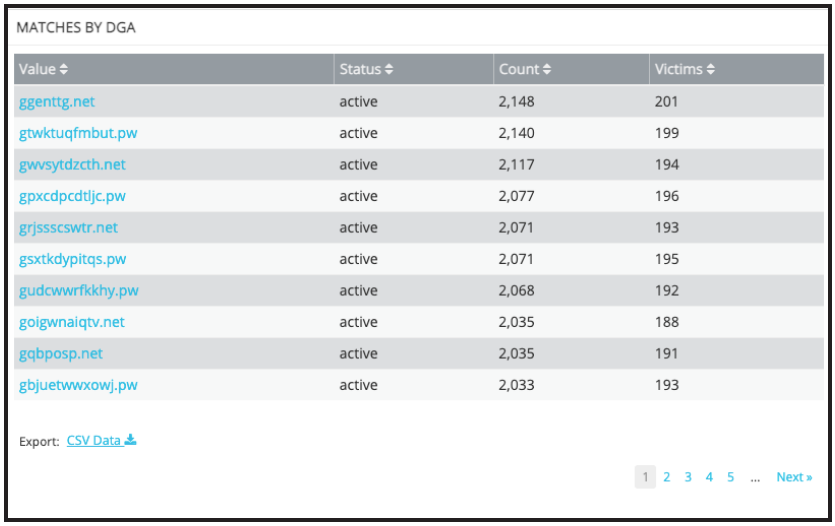
1 2 3 4 5 ... Next »

The following table describes the Matches by Indicator table columns.

Column	Description
Value	The indicator value appearing in event logs. Values in this column are hyperlinks. • Right-click an indicator value and select **Search in ThreatStream**, **Search in VirusTotal**, or **Suppress this Indicator**. You can review the suppressed iTypes on the Manage > Exclude List page. See "Manage the Suppressed Indicators List" on page 273. • Click an indicator value to issue an IOC Match search on the Activity page, filtered for the selected indicator value.
Count	Total event log matches for this indicator during the selected time period.
Victims	The highest daily count of systems or hosts that were impacted by the indicator during the selected time period.
Feed	Number of intelligence feeds that had identified the indicator.

Matches by DGA

This panel displays a table summarizing matches for events related to Domain Generated Algorithm (DGA) domains. See "About DGA Match Searches" on page 95 for an overview of DGAs.


MATCHES BY DGA

Value	Status	Count	Victims
ggenttg.net	active	2,148	201
gtwktuqfmbut.pw	active	2,140	199
gwvsytdzcth.net	active	2,117	194
gpxcdpcdtljc.pw	active	2,077	196
grjsssscswtr.net	active	2,071	193
gsxtkdypitqs.pw	active	2,071	195
gudcwwrfkkhy.pw	active	2,068	192
goigwnaiqtv.net	active	2,035	188
gqbposp.net	active	2,035	191
gbjuetwwxowj.pw	active	2,033	193

Export: CSV Data

1 2 3 4 5 ... Next »

The following table describes the Matches by DGA table columns.

Column	Description
Value	Domain identified as a DGA domain. Values in this column are hyperlinks. • Right-click a DGA value and select **Search in Whois XML** or **Mark as false positive**. You can review the list of domains marked as DGA false positives on the Manage > Exclude List page. See "Manage the DGA Exclude List" on page 276. • Click a DGA value to issue an DGA Match search on the Activity page, filtered for the selected DGA value.
Status	• **active**—High probability the domain was generated with a DGA. • **false positive**—Identified by your analysts as a false positive.
Count	Total event log matches for this DGA domain during the selected time period.
Victims	The highest daily count of systems or hosts that were impacted by the DGA domain during the selected time period.

Chapter 3: Searching Anomali Security Analytics Activity Databases

The Activity pages provide a user interface for searching matched events, as well as imported intelligence or asset data.

Getting Started with Activity Search

The Activity pages provide a user interface for searching matched events, as well as imported intelligence or asset data.

> **Note:** Security Analytics Activity Search is separate from AQL Search. For information about AQL Search, go to the AQL Search Help Center.

Activity Search Indexes

The Activity search menu has a number of pages that can be used to perform searches against different Security Analytics data sets. The following table summarizes the purpose of each.

Activity Search Page	Purpose
IOC Match	Search the IOC Match index. When your event logs are ingested, the Security Analytics correlation engine analyzes those fields in your logs which contain data that can could potentially match IOCs. If the evaluation produces matches, the event log is enriched with your asset data and indexed for activity search. See "Modifying IOC Correlation Engine Settings" on page 349 for details. When you search this index, you can specify as search terms any of the threat intelligence fields and event log fields—or a combination of them. See "IOC Match Activity Searches" on page 68.

Activity Search Page	Purpose
DGA Match	Search the DGA Match index. The DGA Match index is populated by the Security Analytics DGA processor, which analyzes domain data present in event logs during log ingestion to determine the probability a domain is a DGA domain. See "DGA Match Activity Searches" on page 94.
Threat Model — Actor, Attack Pattern, Campaign, Threat Bulletin, TTP, Vulnerability	Search the Threat Model index. The Threat Model index is a view of matches filtered by threat model entity. When you search this index, you search by threat model entity fields. When you view a Security Analytics result details page, the record includes event log details for the match. Refer to the following topics for details about activity search for a particular threat model index: • "Actor Activity Searches" on page 112 • "Attack Pattern Activity Searches" on page 122 • "Campaign Activity Searches" on page 133 • "Threat Bulletin Activity Searches" on page 144 • "TTP Activity Searches" on page 155 • "Vulnerability Activity Searches" on page 167
Asset	Search the Asset index. Asset details are available only if your organization has imported asset data. See "Managing Asset Data Imports" on page 321 and "Asset Activity Searches" on page 202.
Alert	Search the Alert index. The Alert index is populated by the alert engine. In the Alerts results table, the title column shows the name of the alert configuration that generated the alert. See "Alerts Activity Searches" on page 180.

Full-Text Search

A *full-text search* specifies a string that may exist in any column in the targeted Security Analytics index. Full-text searches have the following rules:

- Use single quotes to specify literal matches. Literal matches return records with case-senstive, whole word matching strings. For example, specifying `'apt'` returns only matches with columns having that literal string.
- Use asterisks marks to specify stem pattern matches. Stem pattern matches return records that include the matching string and may have additional characters before or after the stem. For example, specifying specifying `*apt` returns matches with columns containing the string `mapt`; specifying `apt*` returns matches with columns containing the string `aptt`.
- If you do not use single quotes or asterisks marks, the search term is transformed as if you had specified an asterisks following the stem. For example: `apt*`. This means you can possibly get values like `aptt`.

Keyword Search

A *keyword search* specifies a domain or IP address that may exist in any column that has domain or IP address values. For example: `example.com` or `10.1.123.10`. You can use logical operators to form complex search expressions. Keyword searches have the following rules:

- You can specify wildcard characters in search keywords. For example, `10.1.23.*`.
- To search for a keyword that includes spaces, special characters such as period (.) or slash (/), or double-byte characters, enclose the keyword in double quotes (" "). For example, to search for a string with special characters like `http://mydomain.com`, specify `"http://mydomain.com"`. Similarly, to search for the phrase `my domain`, specify `"my domain"`.
- When two or more keywords are specified without an operator, the OR operator is assumed.

Field-Based Search

A *field-based search* specifies *name=value* pairs, where *name* is the column name and *value* is the data expected in that column. For example, to search for indicator matches with Very High severity, enter `severity=very-high` or to search for events tagged with `mirai`, enter `detail=mirai`. For a list of supported fields for each type of search, click the icon to the right of the search query text box. Field-based searches have the following rules:

A *field-based search* specifies *name=value* pairs, where *name* is the column name and *value* is the data expected in that column. For example, to search for indicator

matches with Very High severity, enter `severity=very-high` or to search for events tagged with `mirai`, enter `detail=mirai`. For a list of supported fields for each type of search, click the icon to the right of the search query text box.

Field-based searches have the following rules:

- Wildcard characters and regular expression queries are supported. The regular expression queries follow the Lucene search syntax.
- Spaces and hyphens (-) are treated as word boundaries. For example, a search for `severity = very-high` returns results where the value for severity includes the words `very` or `high`.
- If the field value contains spaces, special characters such as period (.) or slash (/), or double-byte characters, you can use a phrase search expression to match values having all words in the phrase in the order specified. For example, a search for `severity = "very-high"` matches results that have the terms `very` and `high` in that order. To create a phrase search expression, enclose the value in double quotes (" "). A phrase search uses the equals (=) operator. You cannot use contains, startswith, or endswith operators.
- The hyphen is treated as a word boundary, but the underscore (_) is not treated as a word boundary. For example, the value `pub-ts` is treated as two separate words, but the value `pub_ts` is treated as one contiguous word.
- A search with the `startswith`, `endswith`, or `contains` operator matches any word in the value that starts with, ends with, or contains the specified pattern. For example, `tags startswith ts` matches values `pub ts` and `pub-ts` but not `pub_ts`.
- A search for a phrase in quotes with the equals operator matches a value having the phrase words in the same order. For example, `tags = "panama papers"` matches tags like `"abc-panama-papers-xyz"` but not tags like `"abc-papers-panama-xyz"`.
- **Best Practice**: Searching `tags` and `detail` can be challenging. You might have to test and refine the logic of your search expression a few times until you are confident that the results are filtered appropriately for your ad hoc and automated threat hunting tasks. It can help to review the naming conventions that your organization follows for tags, so tagging and searching efforts are well coordinated.

- You can use logical operators (AND, OR, NOT), and parenthetical expressions using () to join together multiple search conditions. For example, `(c2_ip AND ip = 192.168.10.20) OR (brute_ip AND ip = 192.168.10.20)`.
- Use the IN operator to search in string and numeric fields containing a list of values. For numeric lists, float and double values are not supported. Lists being searched must not be empty. You can use `in`, `In`, or `IN`; but not `iN`.

  For string fields, use double quotes to escape special characters.
- *Multi-type fields* are fields that Security Analytics indexes as both *text* and *keyword* field types.
  - Text

    Data for the text type is passed through an analyzer that tokenizes string values. This means string values are broken down into individual terms during indexing to allow for partial matching. Spaces and hyphens (-) are treated as word boundaries.

    For example, when you specify `severity startswith high`, you will notice results where severity is `very-high` or `high`. This is expected for the text type value. During indexing, the value `very-high` is broken into terms `very` and `high`.
  - Keyword

    Data for the keyword type is not transformed during indexing. Therefore, you can assume you are searching a string exactly as found in the raw event log or raw intelligence data. To search the keyword type, append the suffix `.raw` to the fieldname when you form your search expression. Follow the format `fieldname.raw`.

    For example, a search for `event.parent_image.raw contains "C:\Windows"` can match the Windows pathname, including special characters.

    Another useful example is the field `severity.raw`. When you specify `severity.raw startswith high`, you will notice that your result set has only rows where severity is `high`.

    Lastly, compare the following search expressions:

    ```
    event.dest endswith privacy-yahoo.com
    ```

```
event.dest.raw endswith privacy-yahoo.com
```

The fist returns results where the `event.dest` field ends with tokenized terms `privacy` or `yahoo.com`.

The second returns results where the `event.dest.raw` field ends with the raw string `privacy-yahoo.com`.

The following table lists the multi-type fields. To search the keyword type, append the suffix `.raw` to the fieldname when you form your search expression.

Field Source	Field
Asset	asset_dest_dept, asset_dest_hostname, asset_dest_location, asset_dest_vulnerability, asset_src_dept, asset_src_hostname, asset_src_location, asset_src_vulnerability
Intelligence	country, indicator, itype, maltype, org, severity, source, url
Events	event.action, event.answer, event.app, event.category, event.command_line, event.dest, event.event_name, event.file_name, event.file_path, event.host, event.http_referrer, event.message_id, event.original_file_name, event.parent_command_line, event.parent.image, event.platform, event.query, event.receiver, event.record_type, event.reg_key, event.reg_value_data, event.value_name, event.sender, event.sourcetype, event.src, event.subject, event.title, event.url, event.user, event.user_agent, src_host

Search Raw Events

A *raw event* search targets logs collected from specific Link or log sources. Specify the `peek` command and Link ID or the `sourcetype` ID.

Note:

- The `peek` command is only used in searches for raw events. The command does not apply to other searches such as for filter conditions.

- This technique is useful to troubleshoot cases when you want to determine whether a Link is actively forwarding events to Anomali Security Analytics.

To search raw events:

1. Copy the Link ID:
   a. Click the Settings icon in the left navigation panel and select **Security Analytics**.
   b. Click **Links**. This displays all configured Links.
   c. Select the Link ID text and copy it to the clipboard.
2. Go to the **IOC Match** search page to issue a search.
   In the search field, use the following examples as a guide:

   ```
   peek dcid=<paste the Link ID you copied earlier>
   ```

   ```
   peek dcid=9*
   ```

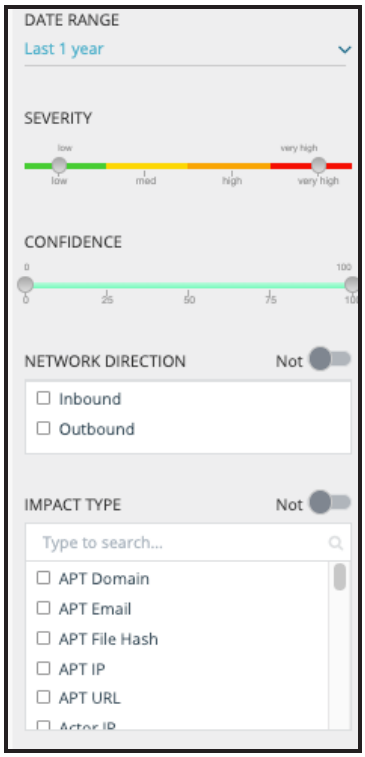
   ```
   peek sourcetype=<name of sourcetype>
   ```

   For example, `peek sourcetype=cisco:sourcefire`.
3. Combine the search expression with other search terms and apply filters, such as time range, to narrow your results.

   Search results default to 10K.

Filter UI

You can use the filter UI in the left pane to specify date range filters and other filters. The types of other filters available vary according to what is appropriate for the targeted Security Analytics index type.



Date Range Filter

The date range specified on Activity search pages filters search results based on dates most pertinent to the index type, as follows.

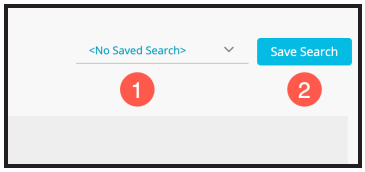
Activity Search Index	Date Filter
IOC Match, DGA Match	Filters by event timestamp.
Actor, Campaign, Threat Bulletin, TTP, Vulnerability	Filters by ThreatStream publication timestamp.
Alert	Filters by alert trigger timestamp.
Asset	Filters by asset record timestamp (the time the asset data was imported into Security Analytics).

Notes:

- The default time range is specified in My Profile settings. See "Change the Default Date Range Filter" on page 293.
- If you change the time period, the time period that you specify persists across all Dashboard and Activity search pages until you change it again or log out of your browser session.

Saved Searches

Saved searches are previously defined search expressions defined by analysts in your organization.



1	Select a previously saved search.
2	Create a new saved search.

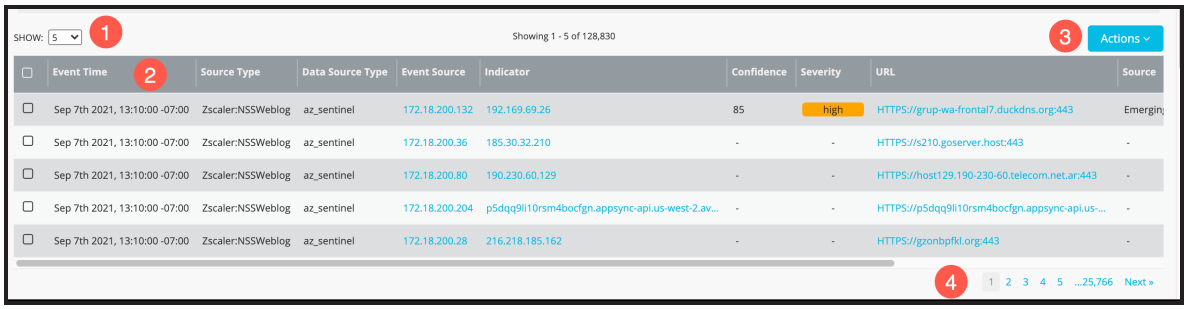
Your organization can maintain saved searches to retrieve and run frequently used or complex queries at the click of a button. The saved queries can be selected to filter the Dashboards visualizations and also be used for configuring Alerts.

To save a search:

1. Refine your search query.
2. Click the **Save Search** button to the right of the search box.
3. Enter a meaningful name and description for the query you are saving.
4. Click **Save**.

Search Result Fields

The search results populate a search results table. You can adjust the rows and columns as shown in the following figure.



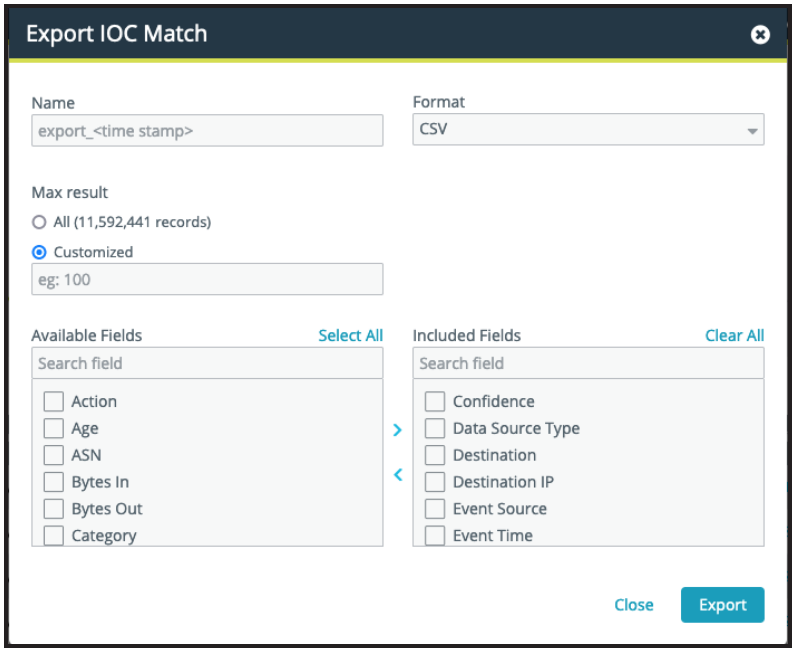
1	Select a number of rows per page.
2	Click the column header to sort the rows in ascending or descending order according to values in the column. Click a column header divider and drag it to make a column wider or more narrow.
3	Use the action menu to configure fields (columns) displayed in the table.
4	Go to the next page of results or another page by page number.

Export Search Results

You can export search results to a file in CSV or JSON format.

To export search results:

1. Click the Export icon above the results table to display the Export dialog box.



2. Enter the following information:
   - **Name**: Name of the export file.
   - **Format**: CSV or JSON.
   - **Max result**: Number of results that should be exported. You can select from **All** or **Customized**. When you select **Customized**, you are prompted to enter the number of results you want to export. Recommended limit is < 1 million results.
3. The default fields to be included in the export are listed under **Included Fields**. Specify the fields to be included or excluded in the export, with one of these options:
   - Select a field and use the **>** or **<** control to move it from one list to another. Repeat as required.
   - Click **Select All** and then click the **>** control to move all **Available Fields** to the **Included Fields** list.

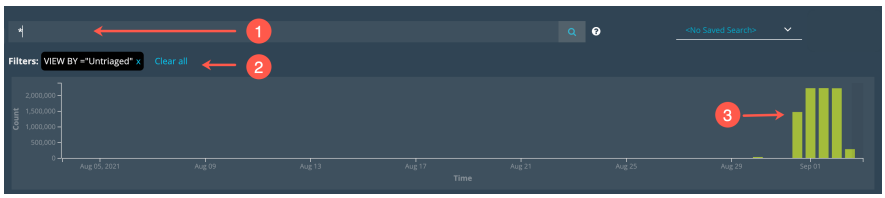
- Click **Clear All** to clear the current list of **Included Fields**. Then you can start with a new list of fields to include.

4. Click **Export**.

   The file is downloaded to your local computer. In addition, you can find the file under **Manage** > **Exports**. All exported files from Anomali Security Analytics are available on this page.

IOC Match Activity Searches

Search the IOC Match index to examine events logs that matched the indicators of compromise (IOC) provided by your threat intelligence feeds.



1	**Search text box**: Specify a keyword or field-based search expression. Keyword searches match any field. Specify field-based name-value pairs for more precise targeting.
2	**Applied Filters**: Review and clear filters.
3	**Matches Timeline**: Click a bar to filter by date. Click and drag over two or more bars to set a date range filter.

About IOC Match Searches

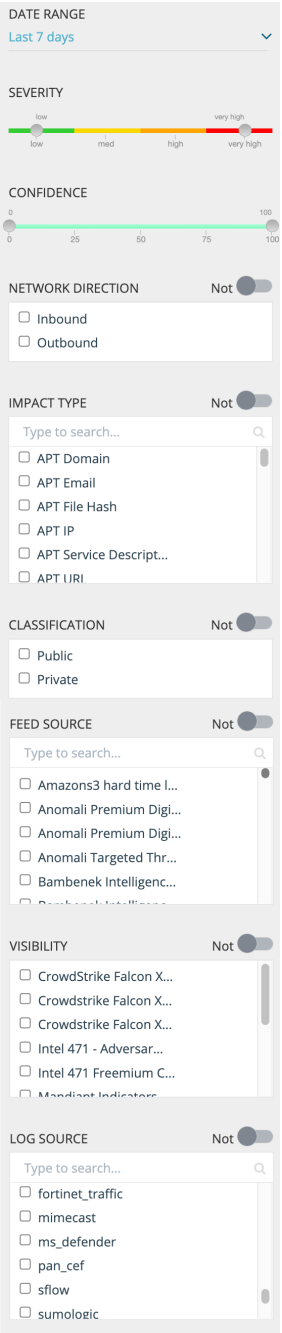
Your organization subscribes to ThreatStream intelligence feeds that make up the set of IOCs that your organization is interested in tracking. The set of indicators are correlated with event logs when the logs are ingested. The correlated rows have both the event log fields and the threat intelligence fields. This enriched data set facilitates security analyst investigations.

During correlation, Security Analytics identifies indicators in newly received event logs. The event logs may include events forwarded from recent activity or from activity that occurred during a backfill period, depending on your Link configuration. A backfill period is an optional setting that enables the Anomali Link to ingest events from a time period before the Link was set up and activated.

IOC Match index searches are vast, but the Activity workbench has tools that make it easy for you to refine search attributes and get a targeted set of results. You can use the filter user interface (UI), as well as more advanced field-based filter expressions.

Filter UI

You can use the filter UI to apply the following filters to your search:



- **Date Range**
  Select a time period, a relative expression, or a date range. The time period filter is based on event time; in other words, the timestamp in the event log.
- **Severity**
  Use the slider to specify an event severity range or drag both ends of the slider to a single severity to filter on just one. Event severity is determined by the indicator that matched the event log.
- **Confidence**
  Use the slider to specify a confidence score range. Confidence score indicates the certainty that an observable exhibits or is connected to malicious behavior. Confidence score is set by a ThreatStream machine learning algorithm that takes many factors into account, but can be overridden by analysts.
- **Network Direction**
  Filter by **Inbound** or **Outbound**. Inbound and outbound are designated from the perspective of the event log source.
- **Impact Type**
  Select an impact type. Impact type refers to the impact designated by the intelligence feed.
- **Classification**
  Filter according to the classification designated by the intelligence feed.
- **Feed Source**
  Select one or more intelligence feed sources.
- **Visibility**
  Select one or more trusted circle names. Trusted circles are organizations with which the ThreatStream observable is shared.
- **Log Source**
  Select one or more event log sources.

> **Note:** You can use negation in search expressions by selecting the **NOT** operator next to the filter heading. For example, to use negation with Log Source, select the sources you do not want to search and toggle on the **NOT** operator next to the Log Source filter heading.

Advanced Filter Expression Examples

The following are a few example filters:

```
state = active AND domain startswith "qq.*"
```

```
state = active AND domain contains "*.ru"
```

```
state = active AND detail=mirai
```

```
state = active AND confidence >= 90
```

```
state = active AND confidence >= 90 AND itype = "apt_ip"
```

```
state = active AND confidence >= 90 AND (severity = "high" OR
severity = "very-high")
```

```
state = active AND confidence >= 90 AND (itype = "apt_ip" OR itype
= "bot_ip" OR itype = "c2_ip")
```

```
state = active AND confidence >= 70 AND (itype startswith "apt" OR
itype startswith "mal" OR itype startswith "c2")
```

```
state = active AND confidence >= 75 AND itype != bot_ip AND itype
!= actor_ip AND itype != brute_ip
```

```
state = active AND ((itype != "bot_ip" AND confidence >= 75) OR
(itype = "bot_ip" AND confidence >= 99)) AND classification =
"public"
```

```
state = active AND event_time >= "2019-01-01T00:00:00"
```

```
state = active AND event.src insubnet "172.18.177.0/24"
```

```
state = active AND (itype=proxy_ip AND indicator insubnet
"70.183.48.0/24")
```

```
NOT indicator insubnet "70.183.48.0/24"
```

```
trusted_circle_ids in [10028, 10029, 10030, 10031]
```

```
(confidence>=60) AND NOT trusted_circle_ids in [123, 456, 789,
890, 901, 121, 324, 356, 677, 888]
```

```
event.event_name != DnsRequest
```

String list:

```
itype in ["scan_ip","c2_domain", "c2_ip"]
```

Numeric list:

```
source_feed_id in [312, 274]
```

For include list information:

```
tags="anomali-include-list-ip"
```

```
tags="anomali-include-list-domain"
```

Filter Operators

The following table describes the logical operators you can use to form complex field-based search expressions. Operator names are **not** case sensitive.

Field Type	Use this Operator
String	=, !=, contains, startswith, insubnet, in (for lists) **Notes:** • The `startswith` operator matches any token in the field that starts with the pattern. For example, the expression `source startswith glass` matches a source field that has the value `Looking Glass C2 - IMDA`. • The `insubnet` operator accepts a value in CIDR notation, enclosed in double quotes (" "). For example, "172.18.177.0/24" • Use double quotes to escape special characters and spaces. Example: `itype in ["scan_ip","c2_domain", "c2_ip"]`
Numeric	=, !=, <, <=, >, >=, in (for lists) For example, `source_feed_id in [312, 274]` **Note:** The `in` operator does not accept float and double types.
Date	=, !=, <, <=, >, >=
Logical	AND, OR, NOT, (*specify a parenthetical expression*)

Filter Fields

In the search box, you can specify keywords or field-value pairs. Keyword searches match any field. Specify field-based name-value pairs for more precise targeting.

The IOC Match table contains three types of fields:

- Event fields: These fields are part of the original event and are denoted by the prefix `event.<field_name>`. For example, `event.dest` denotes the destination IP or hostname of the event.
- Asset fields: These fields are added to the original event by Anomali Security Analytics during correlation. The asset data source is the data your organization provides in scanner reports or CSV files uploaded to Anomali Security Analytics.

Asset fields are denoted by the prefix `asset_<field_name>`. For example, `asset_dest_ip` denotes the IP address for an asset that was the destination in a logged event.

- Enrichment fields: These fields are added to the original event by Anomali Security Analytics during correlation to provide additional intelligence context. For example, itype, which denotes the indicator type of the event.

The following table describes all of the possible IOC Match search fields. The fields listed in the first column correspond with results table column names. The field names listed in the second column are the fields you specify when you form field-based name-value pair search expressions.

> **Note:** Not all fields are included as columns in the results table. When you search by fields without column names, you can locate the matching values in the details page. All of the fields listed in this table can be selected when you export results.

Column Name	Field Name	Type	Description
Age	age	Numeric	Indicates the age of the indicator in days. Event time - intel first seen A negative age value indicates that the event data was added to Anomali Security Analytics through backfill.
Link Type	app_type	String	Link type that generated the event. Possible values: `universal_link`, `splunk`
ASN	asn	String	Autonomous System Number (ASN) for the IP associated with the indicator.
	asset_dest_criticality	String	Criticality associated with the asset that is the destination of a logged event. Possible values: critical, high, medium, low
	asset_dest_dept	String	Assigned department for an asset that is the destination of a logged event. Examples: Engineering, Finance, HR, Labs, Marketing

Column Name	Field Name	Type	Description
	asset_dest_hostname	String	Host name for an asset that is the destination of a logged event. Examples: example.local, example-pc
	asset_dest_ip	String	IP address for an asset that is the destination of a logged event. Example: 192.0.2.1
	asset_dest_location	String	Assigned location for an asset that is the destination of a logged event. Example: Redwood City, CA
	asset_dest_vulnerability	String	Vulnerability CVE number associated with an asset that is the destination of a logged event. Examples: CVE-2021-21137, CVE-2019-3385
Criticality	asset_src_criticality	String	Criticality associated with the asset that is the source of a logged event. Possible values: critical, high, medium, low
Department	asset_src_dept	String	Assigned department for an asset that is the source of a logged event. Examples: Engineering, Finance, HR, Labs, Marketing
Hostname	asset_src_hostname	String	Host name for an asset that is the source of a logged event. Examples: example.local, example-pc
IP	asset_src_ip	String	IP address for an asset that is the source of a logged event. Example: 192.0.2.1
Location	asset_src_location	String	Assigned location for an asset that is the source of a logged event. Example: Redwood City, CA

Column Name	Field Name	Type	Description
Vulnerability	asset_src_vulnerability	String	Vulnerability CVE number associated with an asset that is the source of a logged event. Examples: CVE-2021-21137, CVE-2019-3385
Classification	classification	String	Indicates the confidentiality level of an indicator. Possible values: private, public **Note:** Private also includes Trusted Circles.
Confidence	confidence	Numeric	Score from 0 to 100, as reported by the threat feed provider.
Match Type	corr_type	String	iocmatch
Count	count	Numeric	Aggregated number of events that matched the search criteria.
Country	country	String	Two-letter ISO country code for the IP associated with the indicator. For example, US, CN, DE, and so on.

Column Name	Field Name	Type	Description
Created	date_first	Date	Timestamp of when the indicator was first seen by the threat feed provider. **Notes:** • In the results table, the time displayed is UTC time, adjusted for the browser time zone. • When you form search expressions, specify UTC time in the following format: <YYYY><MM><DD>T<HH>:<MM>:<SS>. The date part and the time part are separated by a capital T. You do not need to include T and the time values if you intend to search by date only. The following is an example of UTC time format: `2022-01-05T00:00:00` • You can also specify a time zone offset for searches where time zone precision is important. In the following example, the time zone offset is the `-08:00` at the end: `2022-01-05T00:00:00-08:00` • In exported results, the date and time are displayed as epoch time values. The following example shows the previous date-time example in epoch format: `1641342478`

Column Name	Field Name	Type	Description
Modified	date_last	Date	Timestamp of when the indicator was last seen by the threat feed provider. **Notes:** • In the results table, the time displayed is UTC time, adjusted for the browser time zone. • When you form search expressions, specify UTC time in the following format: <YYYY><MM><DD>T<HH>:<MM>:<SS>. The date part and the time part are separated by a capital T. You do not need to include T and the time values if you intend to search by date only. The following is an example of UTC time format: `2022-01-05T00:00:00` • You can also specify a time zone offset for searches where time zone precision is important. In the following example, the time zone offset is the `-08:00` at the end: `2022-01-05T00:00:00-08:00` • In exported results, the date and time are displayed as epoch time values. The following example shows the previous date-time example in epoch format: `1641342478`
	dcid	String	ID of the Link from which event was received.
Tags	detail	String	Comments and context associated with the indicator.
Action	event.action	String	*Relevant for firewall and web proxy events* Event log action taken by the source device; for example, `Deny`, `Accept`.

Column Name	Field Name	Type	Description
Answer	event.answer	String	Answers for the DNS query. Example: ["10.10.10.10","10.10.10.11"]
Application	event.app	String	The application detected. Example: Slack, Google Gmail, LinkedIn
Bytes In	event.bytes_in	Numeric	How many bytes received by a network interface. Example: 347
Bytes Out	event.bytes_out	Numeric	How many bytes transmitted by a network interface. Example: 665
Category	event.category	String	*Relevant for AWS VPC and Microsoft Defender logs.* Traffic direction: ingress or egress.
Command Line	event.command_line	String	The full command string of the spawned process. Example: `"\"procdump.exe\" -ma ls"`

Column Name	Field Name	Type	Description
Destination	event.dest	String	Event log destination data. The `event.dest` value populated from event logs is: • An IP address—for example, `192.0.2.1`. • A fully qualified domain name or registered domain name (second-level domain)—for example, `www.google.com` or `google.com`. • Host and domain data extracted from URL data. For example, if Security Analytics receives an event log with a destination URL `http://www.example.com/somepath/34839/jk30jf`, Security Analytics populates `event.dest` with the extracted host and domain `www.example.com`. Indicators that have IP or Domain value types can match `event.dest` values. See "ThreatStream Indicator Types" on page 1028 for a reference that includes indicator value types and descriptions. By default, Security Analytics correlates indicators and `event.dest` values.
Destination IP	event.dest_ip	String	Event log destination IP address. The `event.dest_ip` value populated from event logs is an IP address—for example, `192.0.2.1`. Indicators that have IP value types can match `event.dest_ip` values. See "ThreatStream Indicator Types" on page 1028 for a reference that includes indicator value types and descriptions. By default, Security Analytics correlates indicators and `event.dest_ip` values.

Column Name	Field Name	Type	Description
Destination Port	event.dest_port	Numeric	Event log destination port. Event log destination port field. The value for `event.dest_port` is the port number from the destination host—for example, `80`.
Data Source ID	event.ds_id	Numeric	For Universal Link log sources, this is the log source configuration ID. For Splunk log sources, this field is not applicable.
Data Source Type	event.ds_type	String	Event log data source type. Examples: `az_sentinel`, `qradar`
Event ID	event.event_id	String	A Windows identification number that specifies the event type. Example: 4624
Event Name	event.event_name	String	The name of an event. Example: DnsRequest, ProcessRollup2
Filehash	event.file_hash	String	Event log file hash field. For example, an endpoint management application might write a log that contains file hash values. The `event.filehash` value populated from event logs is a hash value—for example, `69efa658c59d884c0cd6164cbb61d6d0cb0174355dc9c69327dfb76237c9c9c4`. Indicators that have Hash value types can match `event.filehash` values. See "ThreatStream Indicator Types" on page 1028 for a reference that includes indicator value types and descriptions. By default, Security Analytics correlates indicators and `event.filehash` values.
	event.file_hash2	String	A log might have multiple file hash fields.

Column Name	Field Name	Type	Description
	event.file_hash3	String	A log might have multiple file hash fields.
File Name	event.file_name	String	Event log field containing filepath.
File Path	event.file_path	String	The folder containing the file. Sigma name: FilePath Example: C:\Program Files (x86)\VMware\VMware Workstation
Originated Host	event.host	String	Event log hostname field. For example, for events ingested from Splunk Link, the value for `event.host` is the hostname of the Splunk indexer that forwarded the event.
HTTP Method	event.http_method	string	The HTTP method used in the request. Example: get, post, delete, patch
HTTP Referrer	event.http_referrer	string	The HTTP referrer used in the request. Example: https://example.com/ Note: Correlated with indicators of type url.
Image	event.image	String	The executable name of the process. Sigma name: Image, ProcessName, OriginalFileName, TargetImage, TargetFileName Example: svchost.exe
Message ID	event.message_id	String	The globally-unique message identifier. Example: 123e4567-e89b-12d3-a456-426655440000
Original File Name	event.original_file_name	String	Original name of the file that was changed. Example: "test.pdf"

Column Name	Field Name	Type	Description
Parent Command Line	event.parent_command_line	String	The full command string of the parent process. Example: C:\Windows\System32\svchost.exe -k WerSvcGroup
Parent Image	event.parent_image	String	The executable name of the parent process. Example: notepad.exe
Parent Process ID	event.parent_process_id	String	The numeric identifier of the process assigned by the operating system. Example: 4834
Platform	event.platform	String	The operating system of the asset. Sigma name: Platform Example: win, mac, linux
Process ID	event.process_id	Numeric	The numeric identifier of the process assigned by the operating system. Example: 3683
Protocol	event.protocol	String	*Relevant for firewall and web proxy events* Event log protocol field. The value for `event.protocol` is the network protocol used to make the connection to the source device—for example `http`.
DNS Query	event.query	String	The domain that needs to be resolved in a DNS query. Example: www.google.com Note: Correlated with indicators of type domain.

Column Name	Field Name	Type	Description
Email Receiver	event.receiver	String	*Relevant for email-specific events* Event log receiver field. The value for `event.receiver` is the receiver's email address, as specified in the To: field of the email—for example, `user@example.com`. Indicators that have Email value types can match `event.receiver` values. See "ThreatStream Indicator Types" on page 1028 for a reference that includes indicator value types and descriptions. By default, Security Analytics correlates indicators and `event.receiver` values.
Record Type	event.record_type	String	The DNS resource record type. Example: A, CNAME, MX, NS, PTR, AAAA
Registry Key	event.reg_key	string	Registry key that the recorded action was applied to. Sigma name: TargetObject Example: HKEY_LOCAL_MACHINE\SOFTWARE\RegisteredApplications
Registry Value Name	event.reg_value_name	string	Name of the registry value that the recorded action was applied to. Example: "Wordpad"
Registry Value Data	event.reg_value_data	string	Data of the registry value that the recorded action was applied to. Example: Software\Microsoft\Windows\CurrentVersion\Applets\Wordpad

Column Name	Field Name	Type	Description
Email Sender	event.sender	String	*Relevant for email-specific events* Event log sender field. The value for `event.sender` is the sender's email address, as specified in the From: field of the email—for example, `user@example.com`. Indicators that have Email value types can match `event.sender` values. See "ThreatStream Indicator Types" on page 1028 for a reference that includes indicator value types and descriptions. By default, Security Analytics correlates indicators and `event.sender` values.
Source Type	event.sourcetype	String	Source device type that generated the event.
Event Source	event.src	String	Event log source IP field. The `event.src` value populated from event logs is: • An IP address—for example, `192.0.2.1`. • A fully qualified domain name or registered domain name (second-level domain)—for example, `www.google.com` or `google.com`. Indicators that have IP type or Domain value types can match `event.src` values. See "ThreatStream Indicator Types" on page 1028 for a reference that includes indicator value types and descriptions. By default, Security Analytics correlates indicators and `event.src` values.

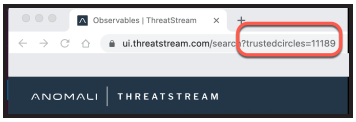
Column Name	Field Name	Type	Description
Source IP	event.src_ip	String	Event log source IP field. The `event.src_ip` value populated from event logs is an IP address—for example, `192.0.2.1`. Indicators that have IP value types can match `event.src_ip` values. See "ThreatStream Indicator Types" on page 1028 for a reference that includes indicator value types and descriptions. By default, Security Analytics correlates indicators and `event.src_ip` values.
Source Port	event.src_port	Numeric	*Relevant for firewall and web proxy events* Event log source port field. The value for `event.src_port` is the port number from the source device from which the connection was made—for example, `3022`.
Subject	event.subject	String	The subject of the message.

Column Name	Field Name	Type	Description
Event Time	event_time	Date	Event log timestamp field. The value for `event.time` is timestamp when the event was generated on the source device—for example, `2021-07-28T19:20:00`. **Notes:** • In the results table, the time displayed is UTC time, adjusted for the browser time zone. • When you form search expressions, specify UTC time in the following format: <YYYY><MM><DD>T<HH>:<MM>:<SS>. The date part and the time part are separated by a capital T. You do not need to include T and the time values if you intend to search by date only. The following is an example of UTC time format: `2022-01-05T00:00:00` • You can also specify a time zone offset for searches where time zone precision is important. In the following example, the time zone offset is the `-08:00` at the end: `2022-01-05T00:00:00-08:00` • In exported results, the date and time are displayed as epoch time values. The following example shows the previous date-time example in epoch format: `1641342478`
Title	event.title	String	Alert title (azure security alert).

Column Name	Field Name	Type	Description
URL	event.url.raw	String	*Relevant for firewall and web proxy events* Event log URL field. The value for `event.url` is populated from URL data having the form `http(s)://<FQDN (registered domain)>:[<port>]/[path]?[<query_params>]`—for example, `http://www.example.com:443/` or `http://www.example.com/somepath/34839/jk30jf`. Indicators that have URL value types can match `event.url` values. See "ThreatStream Indicator Types" on page 1028 for a reference that includes indicator value types and descriptions. By default, Security Analytics correlates indicators and `event.url` values.
User	event.user	String	*Relevant for firewall and web proxy events* Event log user field. The value for `event.user` is the username associated with an authenticated HTTP(S) connection request—for example, `user@example.com`.
User Agent	event.user-agent	String	Event log user agent field. The value for `event.user-agent` is user-agent directive data in an HTTP(S) connection request—for example, `Mozilla/5.0 (platform; rv:geckoversion) Gecko/geckotrail Firefox/firefoxversion`.
Indicator	indicator	String	Value of the indicator. This field contains the value that was matched and is always equal to the value of srcip, url, domain, md5, or email fields.
IOC Type	indicator_type	String	Data type of the indicator. Possible values: ip, domain, url, email, md5

Column Name	Field Name	Type	Description
iType	itype	String	Indicator type. For example, c2_ip, compromised_email, apt_md5, and so on. See "ThreatStream Indicator Types" on page 1028 for a complete list of available indicators.
Latitude	lat	Numeric	Latitude associated with the Geo location of the IP. The value displayed is rounded up to the nearest thousandth decimal place. For example: 32.789. **Note:** Search results are based on non-rounded values, so you might observe anomalous search results, such as a search for `lat = 32.789` does not return a result showing a result value `32.789` but a search for `lat <= 37.789` does show a result for `32.789`. Be aware that rounding produces such minor anomalies.
Longitude	lon	Numeric	Longitude associated with the Geo location of the IP. The value displayed is rounded up to the nearest thousandth decimal place. For example: 16.366. **Note:** Search results are based on non-rounded values, so you might observe anomalous search results, such as a search for `lon = 16.366` does not return a result showing a result value `16.366` but a search for `lon <= 16.366` does show a result for `16.366`. Be aware that rounding produces such minor anomalies.
Malware Family	malware_family	String	One or more public malware family names expected to have originated the domain. **Note:** Malware families are often known by multiple names or aliases. The name shown in the Anomali Security Analytics UI is one of those names or aliases.

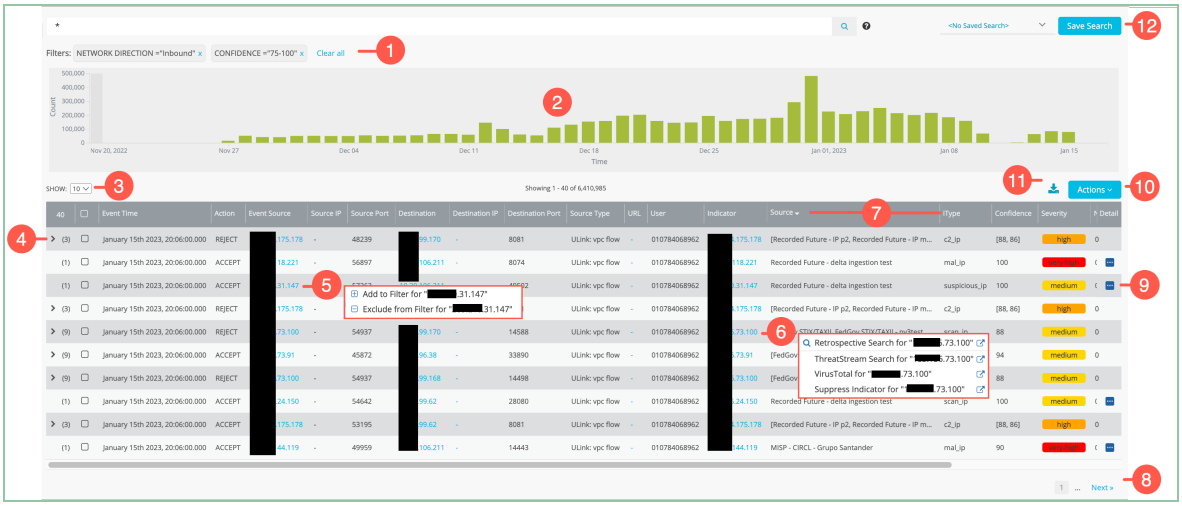
Column Name	Field Name	Type	Description
	originator	Numeric	Indicates whether the connection was inbound or outbound • 0 indicates inbound • 1 indicates outbound
Severity	severity	String	Severity associated with the threat feed that supplied the indicator. Possible values: low, medium, high, very-high **Note:** The search index is tokenized. This means the text is broken down into individual terms during indexing to allow for partial matching. For example, searches for `severity=high` returns matches for both `high` and `very-high`. If the tokenized search behavior returns unexpected results, you can form your search expression for this field using *`fieldname`*`.raw`. For example, if you want results for `high`, not including `very-high`, specify `severity.raw=high`. For more information, see "Getting Started with Activity Search" on page 57.
Source	source.raw	String	Name of the feed provider or organization that reported the indicator.
Feed	source_feed_id	Numeric	Identifier associated with the feed that contained the indicator.
Event Source Host	src_host	String	An event source host value derived from asset_src_hostname, event.src, or event_ip fields, in that order. The hostname provided by the asset enrichment would be most readable, so if it data exists for it, it is used. If not, then the other source fields are evaluated.
State	state	String	Current state of the indicator as reported by the threat feed. Possible values: active, inactive, falsepos

Column Name	Field Name	Type	Description
	trusted_circle_ids	Numeric	ID of the Trusted Circle with which this threat intelligence is shared on ThreatStream. **To find a trusted_circle_ids value to use for Security Analytics search:** 1. In ThreatStream, go to **Manage** > **Trusted Circles**. 2. Click the link in the Name column to display the Observables search page filtered for the selected Trusted Circle. The URL parameter shows the Trusted Circle ID. For example, the following screenshot shows Trusted Circle ID 11189:  In Security Analytics results, the Visibility field on the Details page lists trusted circles data.

IOC Match Results Table

The following figure identifies the UI elements that you use to manipulate the displayed results to find information about IOC matches.

(Click the image to enlarge it.)



1	Review and reset applied filters.
2	Observe the graph of matches over time. Click a bar to filter by date. Click and drag over two or more bars to set a date range filter.
3	Select a number of rows per page.
4	The leftmost column shows the aggregation count for the result row. Click the expander > icon to display the individual result rows. Rows are aggregated when the following fields are identical: `event_time`, `event.action`, `event.src`, `event.src_ip`, `event.src_port`, `event.dest`, `event.dest_ip`, and `event.dest_port`. This occurs when an event log matches more than one indicator or when an indicator has multiple intel source feeds.
5	Option-click a value and select an option to apply a filter that requires or excludes rows matching the value. Not all fields support filtering from the results grid.
6	Click a hyperlinked value and select an option to search ThreatStream, search VirusTotal, run a retrospective search, or add the field value to a Security Analytics Exclude List. The availability of options depend on the data. For example, you can add an indicator value to the Suppressed Indicators list; you can a destination IP address for IP addresses in your local network to the Asset Exclude list.

7	Click the column header to sort the rows in ascending or descending order according to values in the column. Click a column header divider and drag it to make a column wider or more narrow.
8	Go to the next page of results or another page by page number.
9	Display the Details page for the matched event. See "View Match Details" on the next page.
10	Perform an action related to the selected row. See "Perform Actions" below.
11	Export the results table. See "Export Search Results" on page 66.
12	Create a Saved Search configuration. See "Saved Searches" on page 65.

Perform Actions

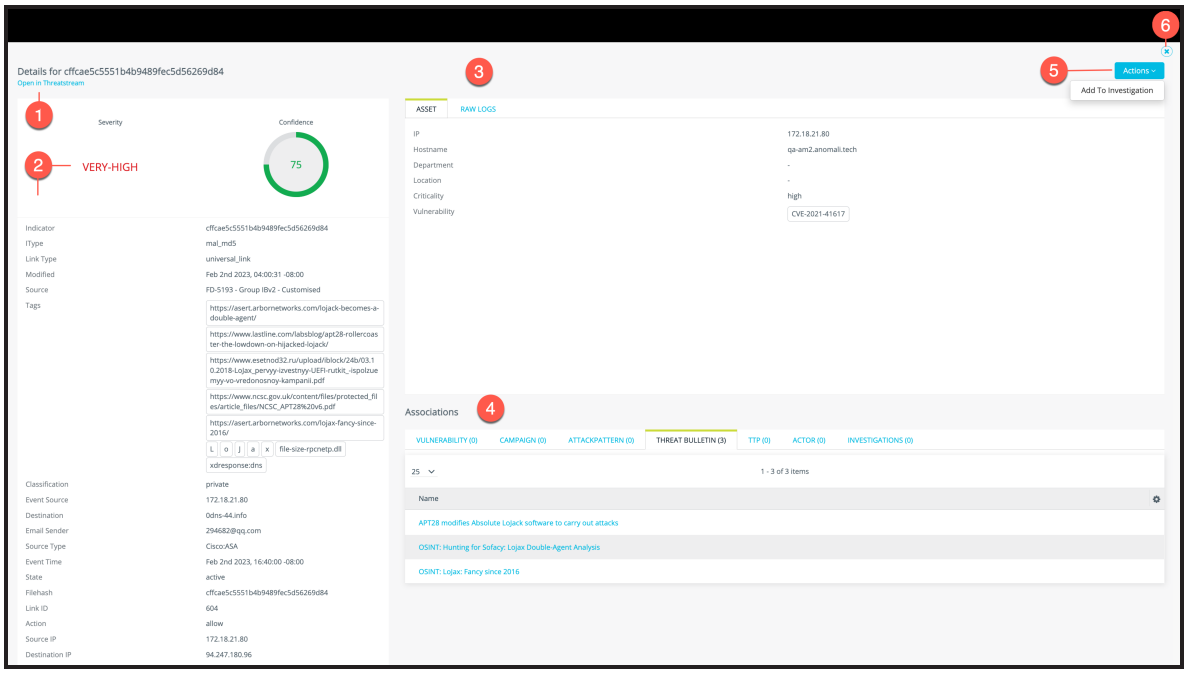
The Action menu above the results table allows you to perform the following actions.

Action	Description
Configure Fields	Select this option to configure the fields (columns) that appear in the results table.
Retrospective Search	Select this option to perform a retrospective search for the indicator correlated with the event.
Investigate	Select this option to add the result to a ThreatStream investigation. Configure one of the following choices: • **Create Investigation**: Specify a name for the investigation and select an assignee to create a ThreatStream investigation. • **Add to Investigation**: Search or browse to find and then select a ThreatStream investigation. **Note:** For information about ThreatStream investigations, refer to the ThreatStream online help.
Suppress Indicators	Select this option to add the indicator to the indicator exclude list.

View Match Details

	Click the Details icon in the right-most column to display the details page.

The following figure identifies the UI elements that you use to find information on the IOC Match Details page.

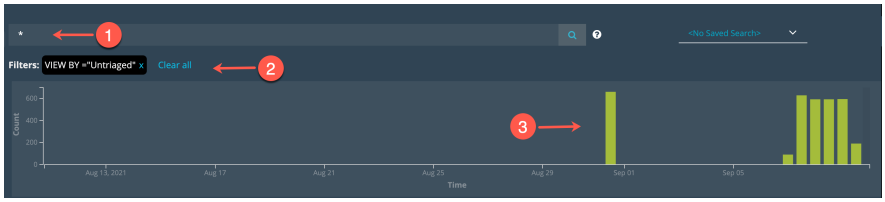


1	Open ThreatStream to view ThreatStream reports about the indicator.
2	Review the indicator details and event details correlated in Security Analytics.

3	Use the tabs to learn more: • **Asset**: View correlated asset details (if applicable). • **Raw Logs**: View more event data. When you click **Get Raw Logs**: ▪ Security Analytics sends a drilldown query to log sources that support drill down queries. The source sends the raw log in response. Raw logs are available as long as they remain available on the log source system. ▪ Security Analytics retrieves event log data from Security Analytics storage for log sources that do not support drilldown queries. The fields in logs stored in Security Analytics have been normalized to Security Analytics event fields. ▪ Security Analytics returns no results if the associated Anomali Link is inactive.
4	Use the tabs to review associated ThreatStream threat model entities and investigations.
5	Click **Actions** and select **Add to Investigation** to add the log to a ThreatStream investigation. **Note:** For information about ThreatStream investigations, refer to the ThreatStream online help.
6	Click the **X** to exit the details page and return to the results table.

DGA Match Activity Searches

Search the DGA Match index to examine events logs that matched domains deemed likely Domain Generated Algorithm (DGA) domains.



1	**Search text box**: Specify a keyword or field-based search expression. Keyword searches match any field. Specify field-based name-value pairs for more precise targeting.
2	**Applied Filters**: Review and clear filters.
3	**Matches Timeline**: Click a bar to filter by date. Click and drag over two or more bars to set a date range filter.

About DGA Match Searches

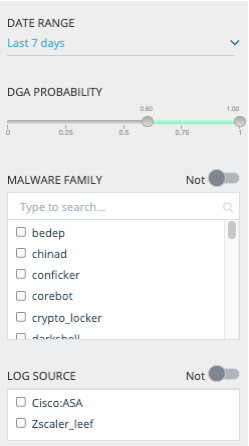
Anomali Security Analytics automatically processes domain names (contained in the host names and URLs) in the events received from your network to determine the likelihood of these being DGA domains. The Anomali Security Analytics DGA processor uses machine learning to calculate the probability of a domain in an event being a DGA domain. Domains with a probability of 60% or higher are considered "likely DGAs". The Security Analytics DGA processor further corroborates the state of a domain against other data sources before classifying the domain state as *active* or *benign*. An active domain has a high probability as generated with a DGA, while a benign domain is most likely not generated by a DGA.

Security Analytics generates matches for active DGA domains. The machine learning engine continuously updates the state of a domain as Security Analytics ingests domain information.

Anomali Security Analytics *does not* generate DGA matches for domains determined to be benign or false positives.

Filter UI

You can use the filter UI to apply the following filters to your search:



- **Date Range**
  Select a time period, a relative expression, or a date range. The time period filter is based on event time; in other words, the timestamp in the event log.

- **DGA Probability**
  Use the slider to specify a DGA probability range.

- **Malware Family**
  Malware family is a name given to multiple file artifacts that have significant code similarities and are distinct enough from other groups of known malware. Malware families are often known by multiple names or aliases. Select one or more malware families.

- **Log Source**
  Select one or more event log sources.

> **Note:** You can use negation in search expressions by selecting the **NOT** operator next to the filter heading. For example, to use negation with Log Source, select the sources you do not want to search and toggle on the **NOT** operator next to the Log Source filter heading.

Filter Examples

The following are a few example filters:

```
dga_prob >= .80
dga_prob > 0.5 AND dga_prob < 0.8
state = active AND event.dest = "qukaheylka.xyz"
event.url.raw="http://tsrs.pw/"
```

```
event.user="barbe_meletius@live.com"
malware_family startswith conficker
malware_family in ["Gameover_DGA", "Emotet.c"]
event.sourcetype contains cisco
dga_prob >= .80 and event.sourcetype != cisco
dga_prob >= .80 and (event.sourcetype = Zscaler or leef)
dga_prob >= .80 and ((event.sourcetype = Zscaler or leef) and
(user !="user6@acme.com"))
```

Filter Operators

The following table describes the logical operators you can use to form complex field-based search expressions. Operator names are **not** case sensitive.

Field Type	Use this Operator
String	=, !=, contains, startswith, insubnet, in (for lists) **Notes:** • The `startswith` operator matches any token in the field that starts with the pattern. For example, the expression `source startswith glass` matches a source field that has the value `Looking Glass C2 - IMDA`. • The `insubnet` operator accepts a value in CIDR notation, enclosed in double quotes (" "). For example, "172.18.177.0/24" • Use double quotes to escape special characters and spaces. Example: `itype in ["scan_ip","c2_domain", "c2_ip"]`
Numeric	=, !=, <, <=, >, >=, in (for lists) For example, `source_feed_id in [312, 274]` **Note:** The `in` operator does not accept float and double types.
Date	=, !=, <, <=, >, >=
Logical	AND, OR, NOT, (*specify a parenthetical expression*)

Filter Fields

The DGA Match table contains two types of fields:

- Event fields: These fields are part of the original event and are denoted by the prefix `event.<field_name>`. For example, `event.dest` denotes the destination IP or hostname of the event.
- Enrichment fields: These fields are added to the original event by Anomali Security Analytics during correlation to provide additional intelligence context. For example, itype, which denotes the indicator type of the event.

The following table describes all of the possible search fields. The fields listed in the first column correspond with results table column names. The field names listed in the second column are the fields you specify when you form field-based name-value pair search expressions.

> **Note:** Not all fields are included as columns in the results table. When you search by fields without column names, you can locate the matching values in the details page. All of the fields listed in this table can be selected when you export results.

Column Name	Field Name	Type	Description
Age	age		Does not apply to the DGA Match index.
	app_type	String	Link type that generated the event.
ASN	asn		Does not apply to the DGA Match index.
	asset_dest_criticality	String	Does not apply to the DGA Match index.
	asset_dest_dept	String	Does not apply to the DGA Match index.
	asset_dest_hostname	String	Does not apply to the DGA Match index.
	asset_dest_ip	String	Does not apply to the DGA Match index.

Column Name	Field Name	Type	Description
	asset_dest_location	String	Does not apply to the DGA Match index.
	asset_dest_vulnerability	String	Does not apply to the DGA Match index.
	asset_src_criticality	String	Does not apply to the DGA Match index.
	asset_src_dept	String	Does not apply to the DGA Match index.
Hostname	asset_src_hostname	String	Does not apply to the DGA Match index.
	asset_src_ip	String	Does not apply to the DGA Match index.
	asset_src_location	String	Does not apply to the DGA Match index.
	asset_src_vulnerability	String	Does not apply to the DGA Match index.
Classification	classification	String	Does not apply to the DGA Match index.
Confidence	confidence	Numeric	Does not apply to the DGA Match index.
Count	count	Numeric	Aggregated number of events that matched the search criteria.
Country	country		Does not apply to the DGA Match index.
Created	date_first	Date	Does not apply to the DGA Match index.
Modified	date_last	Date	Does not apply to the DGA Match index.

Column Name	Field Name	Type	Description
	dcid	String	ID of the Link from which event was received.
Tags	detail	String	Does not apply to the DGA Match index.
DGA Probability	dga_prob	Numeric	Probability based on Anomali Security Analytics's DGA algorithm that the domain in the event is a DGA domain.
DGA TAG	dga_tag	String	Does not apply to the DGA Match index.
Action	event.action	String	*Relevant for firewall and web proxy events* Event log action taken by the source device; for example, `Deny`, `Accept`.
Application	event.app	String	The application detected. Example: ProcDump
Bytes In	event.bytes_in	Numeric	How many bytes received by a network interface. Example: 347
Bytes Out	event.bytes_out	Numeric	How many bytes transmitted by a network interface. Example: 665
Category	event.category	String	*Relevant for AWS VPC and Microsoft Defender logs.* Traffic direction: ingress or egress.
Command Line	event.command_line	String	The full command string of the spawned process. Example: `"\"procdump.exe\" -ma ls"`

Column Name	Field Name	Type	Description
Destination	event.dest	String	Event log destination data. The `event.dest` value populated from event logs is: • An IP address—for example, `192.0.2.1`. • A fully qualified domain name or registered domain name (second-level domain)—for example, `www.google.com` or `google.com`. • Host and domain data extracted from URL data. For example, if Security Analytics receives an event log with a destination URL `http://www.example.com/somepath/34839/jk30jf`, Security Analytics populates `event.dest` with the extracted host and domain `www.example.com`. Indicators that have IP or Domain value types can match `event.dest` values. See "ThreatStream Indicator Types" on page 1028 for a reference that includes indicator value types and descriptions. By default, Security Analytics correlates indicators and `event.dest` values.
Destination IP	event.dest_ip		Event log destination IP address. The `event.dest_ip` value populated from event logs is an IP address—for example, `192.0.2.1`. Indicators that have IP value types can match `event.dest_ip` values. See "ThreatStream Indicator Types" on page 1028 for a reference that includes indicator value types and descriptions. By default, Security Analytics correlates indicators and `event.dest_ip` values.
Destination Port	event.dest_port	Numeric	Does not apply to the DGA Match index.

Column Name	Field Name	Type	Description
	event.ds_id		Does not apply to the DGA Match index.
Data Source Type	event.ds_type	String	Event log data source type. Examples: az_sentinel, qradar
Event ID	event.event_id	String	A Windows identification number that specifies the event type. Example: 4624
Event Name	event.event_name	String	The name of an event. Example: DnsRequest, ProcessRollup2
File Hash	event.file_hash	String	Event log file hash field. For example, an endpoint management application might write a log that contains file hash values. The `event.filehash` value populated from event logs is a hash value—for example, `69efa658c59d884c0cd6164cbb61d6d0cb0174355dc9c69327dfb76237c9c9c4`. Indicators that have Hash value types can match `event.filehash` values. See "ThreatStream Indicator Types" on page 1028 for a reference that includes indicator value types and descriptions. By default, Security Analytics correlates indicators and `event.filehash` values.
	event.file_hash2	String	A log might have multiple file hash fields.
	event.file_hash3	String	A log might have multiple file hash fields.
File Name	event.file_name	String	Does not apply to the DGA Match index.

Column Name	Field Name	Type	Description
Host	event.host	String	Event log hostname field. For example, for events ingested from Splunk Link, the value for `event.host` is the hostname of the Splunk indexer that forwarded the event.
Image	event.image	String	The executable name of the process. Sigma name: Image, ProcessName, OriginalFileName, TargetImage, TargetFileName Example: svchost.exe
Message ID	event.message_id	String	The globally-unique message identifier. Example: 123e4567-e89b-12d3-a456-426655440000
Original File Name	event.original_file_name	String	Original name of the file that was changed. Example: "test.pdf"
Parent Command Line	event.parent_command_line	String	The full command string of the parent process. Example: C:\Windows\System32\svchost.exe -k WerSvcGroup
Parent Image	event.parent_image	String	The executable name of the parent process. Example: notepad.exe
Parent Process ID	event.parent_process_id	String	The numeric identifier of the process assigned by the operating system. Example: 4834
Platform	event.platform	String	The operating system of the asset. Sigma name: Platform Example: win, mac, linux
Parent Process ID	event.parent_process_id	String	The numeric identifier of the process assigned by the operating system. Example: 4834

Column Name	Field Name	Type	Description
Protocol	event.protocol	String	*Relevant for firewall and web proxy events* Event log protocol field. The value for `event.protocol` is the network protocol used to make the connection to the source device—for example `http`.
DNS Query	event.query	String	The domain that needs to be resolved in a DNS query. Example: www.google.com Note: Correlated with indicators of type domain.
Email Receiver	event.receiver	String	Does not apply to the DGA Match index.
Record Type	event.record_type	String	The DNS resource record type. Example: A, CNAME, MX, NS, PTR, AAAA
Registry Key	event.reg_key	string	Registry key that the recorded action was applied to. Sigma name: TargetObject Example: HKEY_LOCAL_MACHINE\SOFTWARE\RegisteredApplications
Registry Value Name	event.reg_value_name	string	Name of the registry value that the recorded action was applied to. Example: "Wordpad"
Registry Value Data	event.reg_value_data	string	Data of the registry value that the recorded action was applied to. Example: Software\Microsoft\Windows\CurrentVersion\Applets\Wordpad

Column Name	Field Name	Type	Description
Email Sender	event.sender	String	*Relevant for email-specific events* Event log sender field. The value for `event.sender` is the sender's email address, as specified in the From: field of the email—for example, `user@example.com`. Indicators that have Email value types can match `event.sender` values. See "ThreatStream Indicator Types" on page 1028 for a reference that includes indicator value types and descriptions. By default, Security Analytics correlates indicators and `event.sender` values.
Source Type	event.sourcetype	String	Source device type that generated the event.
Event Source	event.src	String	Event log source IP field. The `event.src` value populated from event logs is: • An IP address—for example, `192.0.2.1`. • A fully qualified domain name or registered domain name (second-level domain)—for example, `www.google.com` or `google.com`. Indicators that have IP type or Domain value types can match `event.src` values. See "ThreatStream Indicator Types" on page 1028 for a reference that includes indicator value types and descriptions. By default, Security Analytics correlates indicators and `event.src` values.
Source IP	event.src_ip	String	Does not apply to the DGA Match index.
Source Port	event.src_port	Numeric	Does not apply to the DGA Match index.

Column Name	Field Name	Type	Description
Event Time	event_time	Date	Event log timestamp field. The value for `event.time` is timestamp when the event was generated on the source device—for example, `2021-07-28T19:20:00.000Z`. **Notes:** • In the results table, the time displayed is UTC time, adjusted for the browser time zone. • When you form search expressions, specify UTC time in the following format: <YYYY><MM><DD>T<HH>:<MM>:<SS>. The date part and the time part are separated by a capital T. You do not need to include T and the time values if you intend to search by date only. The following is an example of UTC time format: `2022-01-05T00:00:00` • You can also specify a time zone offset for searches where time zone precision is important. In the following example, the time zone offset is the `-08:00` at the end: `2022-01-05T00:00:00-08:00` • In exported results, the date and time are displayed as epoch time values. The following example shows the previous date-time example in epoch format: `1641342478`
Title	event.title	String	Alert title (azure security alert).

Column Name	Field Name	Type	Description
URL	event.url.raw	String	*Relevant for firewall and web proxy events* Event log URL field. The value for `event.url` is populated from URL data having the form `http(s)://<FQDN (registered domain)>:[<port>]/[path]?[<query_params>]`—for example, `http://www.example.com:443/` or `http://www.example.com/somepath/34839/jk30jf`. Indicators that have URL value types can match `event.url` values. See "ThreatStream Indicator Types" on page 1028 for a reference that includes indicator value types and descriptions. By default, Security Analytics correlates indicators and `event.url` values.
User	event.user	String	*Relevant for firewall and web proxy events* Event log user field. The value for event.user is the username associated with an authenticated HTTP(S) connection request—for example, `user@example.com`.
User Agent	event.user-agent	String	Does not apply to the DGA Match index.
Indicator	indicator	String	Value of the indicator. This field contains the value that was matched and is always equal to the value of srcip, url, domain, md5, or email fields.
	indicator_type	String	Data type of the indicator. Possible values: ip, domain, url, email, md5
iType	itype	String	Does not apply to the DGA Match index.
Latitude	lat	Numeric	Does not apply to the DGA Match index.

Column Name	Field Name	Type	Description
Location	loc		Does not apply to the DGA Match index.
Longitude	lon	Numeric	Does not apply to the DGA Match index.
Malware Family	malware_family	String	One or more public malware family names expected to have originated the domain. **Note:** Malware families are often known by multiple names or aliases. The name shown in the Anomali Security Analytics UI is one of those names or aliases.
	originator	Numeric	Indicates whether the connection was inbound or outbound • 0 indicates inbound • 1 indicates outbound
Severity	severity	String	Does not apply to the DGA Match index.
	source.raw	String	Does not apply to the DGA Match index.
Feed	source_feed_id	Numeric	Does not apply to the DGA Match index.
Event Source Host	src_host	String	An event source host value derived from the event.src field.
State	state	String	Current state of the domain either as determined by the Anomali Security Analytics's DGA engine or marked by user. Possible values: active, benign, falsepos
	trusted_circle_ids	Numeric	Does not apply to the DGA Match index.

Column Name	Field Name	Type	Description
	trusted_ circle_ names	Strin g	Does not apply to the DGA Match index.

DGA Match Results Table

The following figure identifies the UI elements that you use to manipulate the displayed results to find information about DGA matches.

1	Review and reset applied filters.
2	Observe the graph of matches over time.
3	Select a number of rows per page.
4	Click the column header to sort the rows in ascending or descending order according to values in the column. Click a column header divider and drag it to make a column wider or more narrow.
5	Go to the next page of results or another page by page number.
6	Export the results table. See "Export Search Results" on page 66.

7	Perform an action related to the selected row. See "Perform Actions" below.
8	Click a hyperlinked value and select an option to run a Security Analytics retrospective search or search VirusTotal.
9	Display the Details page for the matched event. See "View Match Details" below.
10	Create a Saved Search configuration. See "Saved Searches" on page 65.

Perform Actions

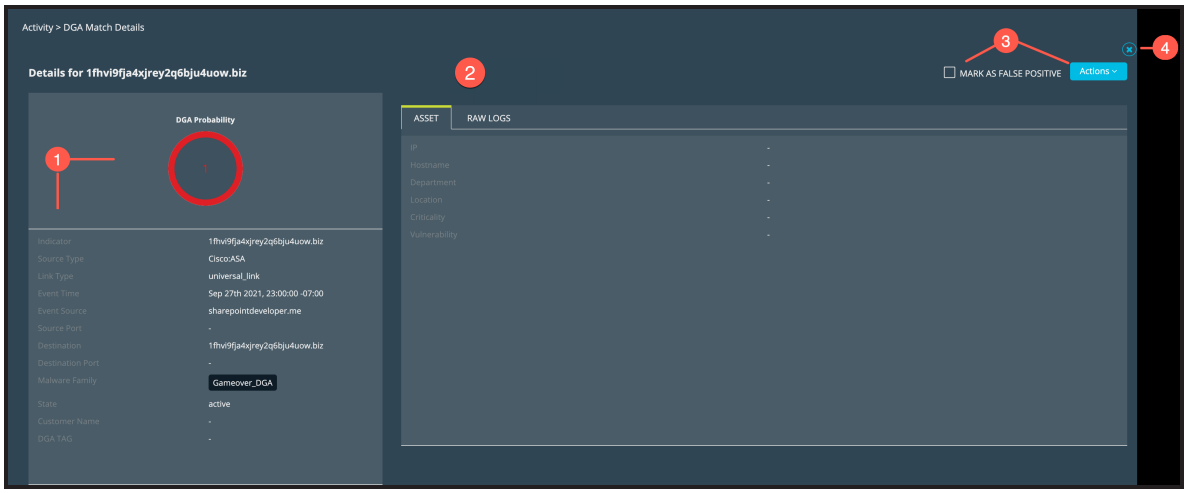
The Action menu above the results table allows you to perform the following actions.

Action	Description
Configure Fields	Select this option to configure the fields (columns) that appear in the results table.
Retrospective Search	Select this option to perform a retrospective search for the indicator correlated with the event.
Investigate	Select this option to add the result to a ThreatStream investigation. Configure one of the following choices: • **Create Investigation**: Specify a name for the investigation and select an assignee to create a ThreatStream investigation. • **Add to Investigation**: Search or browse to find and then select a ThreatStream investigation. **Note:** For information about ThreatStream investigations, refer to the ThreatStream online help.
Mark As False Positive	Select this option to add the indicator to the DGA exclude list.

View Match Details

•••	Click the Details icon in the right-most column to display the details page.

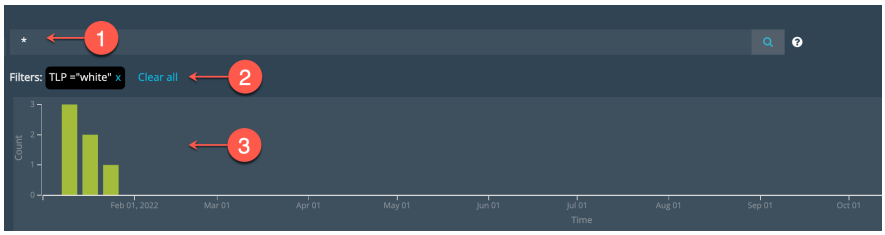
The following figure identifies the UI elements that you use to find information on the DGA Match Details page.



1	Review the indicator details and event details correlated in Security Analytics.
2	Use the tabs to learn more: • **Asset**: View correlated asset details (if applicable). • **Raw Logs**: View more event data. When you click **Get Raw Logs**: ▪ Security Analytics sends a drilldown query to log sources that support drill down queries. The source sends the raw log in response. Raw logs are available as long as they remain available on the log source system. ▪ Security Analytics retrieves event log data from Match storage for log sources that do not support drilldown queries. The fields in logs stored in Match have been normalized to Match event fields. ▪ Security Analytics returns no results if the associated Anomali Link is inactive.
3	Select **Mark As False Positive** or click **Actions** and select **Add to Investigation** to add the log to a ThreatStream investigation. **Note:** For information about ThreatStream investigations, refer to the ThreatStream online help.
4	Click the **X** to exit the details page and return to the results table.

Actor Activity Searches

Search the Actor index to examine Threat Actors provided by threat intelligence feeds that have matched event logs during the specified time period.



1	**Search text box**: Specify a keyword or field-based search expression. Keyword searches match any of the following fields: name, feed source, and tags. Specify field-based name-value pairs for more precise targeting.
2	**Applied Filters**: Review and clear filters.
3	**ThreatStream Publication Timeline**: Bars indicate when the threat entity publication was last modified in ThreatStream. Click a bar to filter by date. Click and drag over two or more bars to set a date range filter.

About Actor Searches

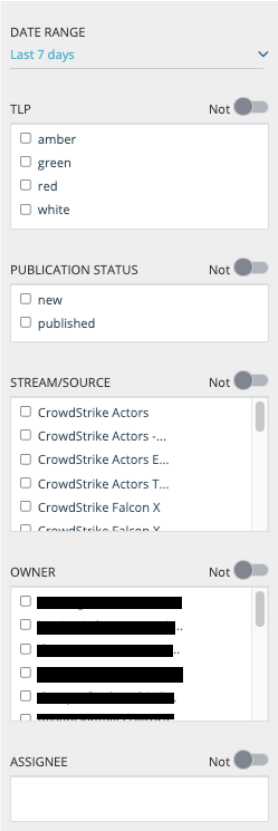
The Anomali Threat Model is STIX-compatible and supports workflows for developing threat intelligence using a commonly understood taxonomy of threat entities. Security Analytics has a search index for the following threat model entities: Actors, Attack Patterns, Campaigns, TTPs, Threat Bulletins, and Vulnerabilities.

An *Actor* is a threat entity that refers to the individuals and organizations reputed to operate with malicious intent.

When you search the Threat Model index, you search by threat model entity fields. When you view a Security Analytics result details page, the record includes event log details for the match.

Filter UI

You can use the filter UI to apply the following filters to your search:


DATE RANGE
Last 7 days
TLP
Not
amber
green
red
white
PUBLICATION STATUS
Not
new
published
STREAM/SOURCE
Not
CrowdStrike Actors
CrowdStrike Actors -...
CrowdStrike Actors E...
CrowdStrike Actors T...
CrowdStrike Falcon X
OWNER
Not
ASSIGNEE
Not

- **Date Range**
  Select a time period, a relative expression, or a date range. The time period filter is based on the ThreatStream publication date (the timestamp for "Modified" in ThreatStream).
- **TLP**
  Select a TLP (Traffic Light Protocol) associated with the entity.
- **Publication Status**
  Select a publication status: New, Pending Review, Review Requested, Reviewed, or Published.
- **Stream/Source**
  Select the name of the Feed in ThreatStream.
- **Owner**
  Select the ThreatStream user who created the entity.
- **Assignee**
  Select the ThreatStream user assigned to investigate.

> **Note:** You can use negation in search expressions by selecting the **NOT** operator next to the filter heading. For example, to use negation with TLP, select the values you do not want to search and toggle on the **NOT** operator next to the TLP filter heading.

Filter Examples

```
modified_ts > "2021-11-09T15:50:00"
```

```
publication_status=new and tags=test
```

```
(publication_status = published or new) and feed_name contains
group
```

```
(publication_status != new) and (feed_name contains group or
crowd)
```

```
modified_ts > "2021-11-09T15:50:00" and (publication_status !=
new) and (feed_name contains group or crowd)
```

```
tags in ["GENERAL_TTP:Bot", "ACTOR_TYPE:Nation State"] and
(modified_ts > "2020-12-01")
```

Filter Operators

The following table describes the logical operators you can use to form complex field-based search expressions. Operator names are not case sensitive.

Field Type	Use this Operator
String	=, !=, contains, startswith, in (for lists) **Notes:** • The `startswith` operator matches any token in the field that starts with the pattern. For example, the expression `name startswith spider` matches a source field that has the value `GRACEFUL SPIDER`. • Use double quotes to escape special characters and spaces in searches with `=`, `!=`, and `in` operators. Examples: `name = "GRACEFUL SPIDER"`, `name != "GRACEFUL SPIDER"`, `tags in ["GENERAL_TTP:Bot", "ACTOR_TYPE:Nation State"]`
Numeric	=, !=, <, <=, >, >=, in (for lists) For example, `id in [312, 274]` **Note:** The `in` operator does not accept float and double types.
Date	=, !=, <, <=, >, >=
Logical	AND, OR, NOT, (*specify a parenthetical expression*)

Filter Fields

The following table describes all of the possible Actor search fields. The fields listed in the first column correspond with results table column names. The field names listed in the second column are the fields you specify when you form field-based name-value pair search expressions.

> **Note:** Not all fields are included as columns in the results table. When you search by fields without column names, you can locate the matching values in the details page. All of the fields listed in this table can be selected when you export results.

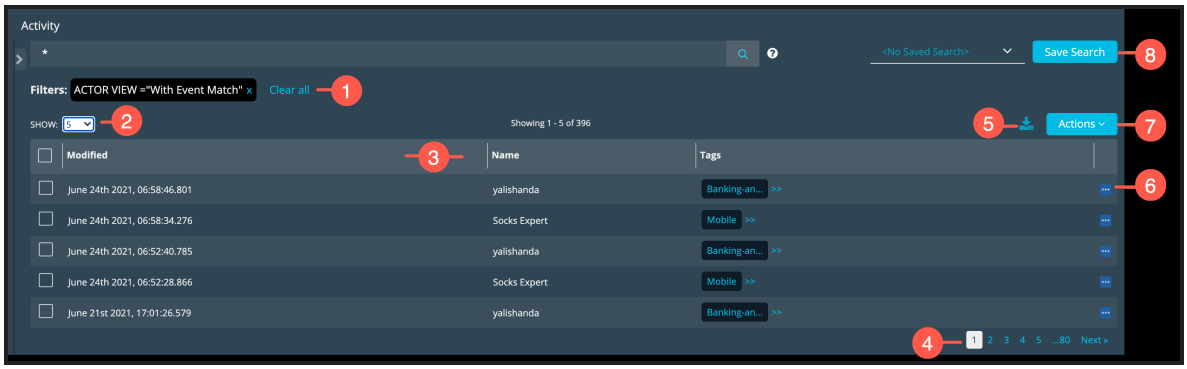
Column Name	Field Name	Type	Description
Assignee	assignee_user	String	User name on ThreatStream who is assigned to investigate.
Created	created_ts	Date	Timestamp of when the entity was created on ThreatStream. **Notes:** • In the results table, the time displayed is UTC time, adjusted for the browser time zone. • When you form search expressions, specify UTC time in the following format: <YYYY><MM><DD>T<HH>:<MM>:<SS>. The date part and the time part are separated by a capital T. You do not need to include T and the time values if you intend to search by date only. The following is an example of UTC time format: `2022-01-05T00:00:00` • You can also specify a time zone offset for searches where time zone precision is important. In the following example, the time zone offset is the `-08:00` at the end: `2022-01-05T00:00:00-08:00` • In exported results, the date and time are displayed as epoch time values. The following example shows the previous date-time example in epoch format: `1641342478`
Stream/Source	feed_name	String	Name of the feed in ThreatStream.

Column Name	Field Name	Type	Description
ID	id	Numeric	Entity ID in ThreatStream.
Modified	modified_ts	Date	Timestamp of when the entity was last updated on ThreatStream. **Notes:** • In the results table, the time displayed is UTC time, adjusted for the browser time zone. • When you form search expressions, specify UTC time in the following format: <YYYY><MM><DD>T<HH>:<MM>:<SS>. The date part and the time part are separated by a capital T. You do not need to include T and the time values if you intend to search by date only. The following is an example of UTC time format: `2022-01-05T00:00:00` • You can also specify a time zone offset for searches where time zone precision is important. In the following example, the time zone offset is the `-08:00` at the end: `2022-01-05T00:00:00-08:00` • In exported results, the date and time are displayed as epoch time values. The following example shows the previous date-time example in epoch format: `1641342478`
Name	name	String	Name of the entity.

Column Name	Field Name	Type	Description
Owner	owner_user	String	Name of the user in the organization on Anomali ThreatStream that created the entity.
Publication Status	publication_status	String	• `new` • `pending_review` • `review_requested` • `reviewed` • `published`
Tags	tags	String	Tags associated with the entity that can be used to search for the entity.
TLP	tlp	String	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. Possible values: white, yellow, green, red

Actor Match Results Table

The following figure identifies the UI elements that you use to manipulate the displayed results to find information about Actor matches.



1	Review and reset applied filters.
2	Select a number of rows per page.
3	Click the column header to sort the rows in ascending or descending order according to values in the column. Click a column header divider and drag it to make a column wider or more narrow.
4	Go to the next page of results or another page by page number.
5	Export the results table. See "Export Search Results" on page 66.
6	Display the Details page for the matched event. See "View Details" on the next page.
7	Perform an action related to the selected row. See "Perform Actions" below.
8	Create a Saved Search configuration. See "Saved Searches" on page 65.

Perform Actions

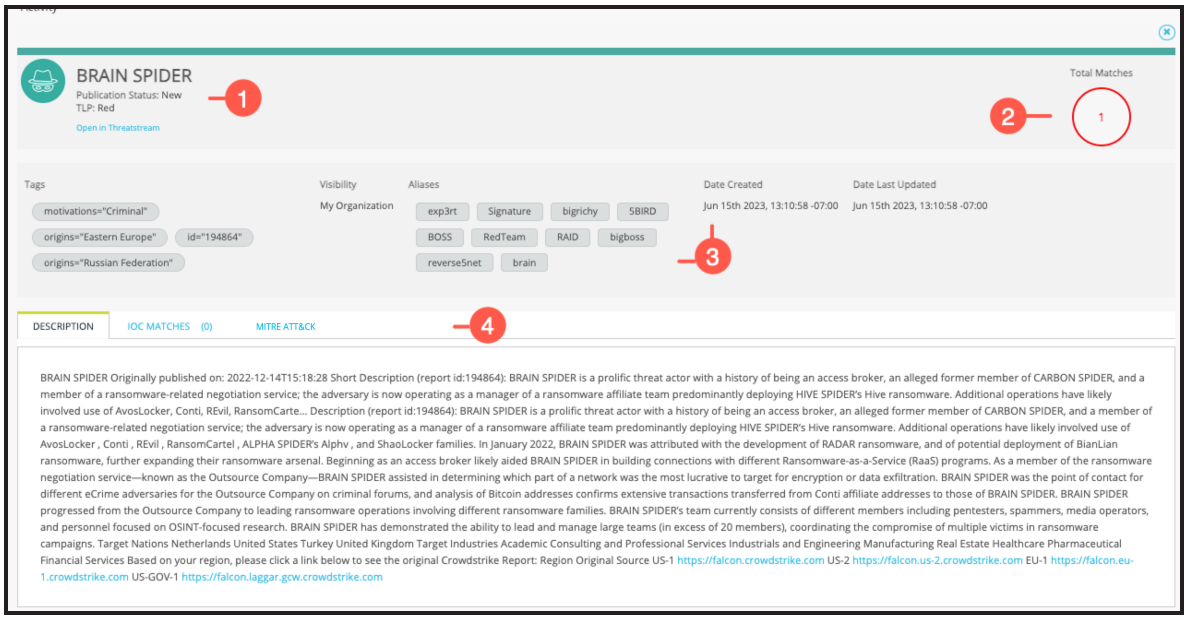
The Action menu above the results table allows you to perform the following actions.

Action	Description
Configure Fields	Select this option to configure the fields (columns) that appear in the results table.
Retrospective Search	Select this option to perform a retrospective search for the indicator correlated with the event.

View Details

•••	Click the Details icon in the right-most column to display the details page.

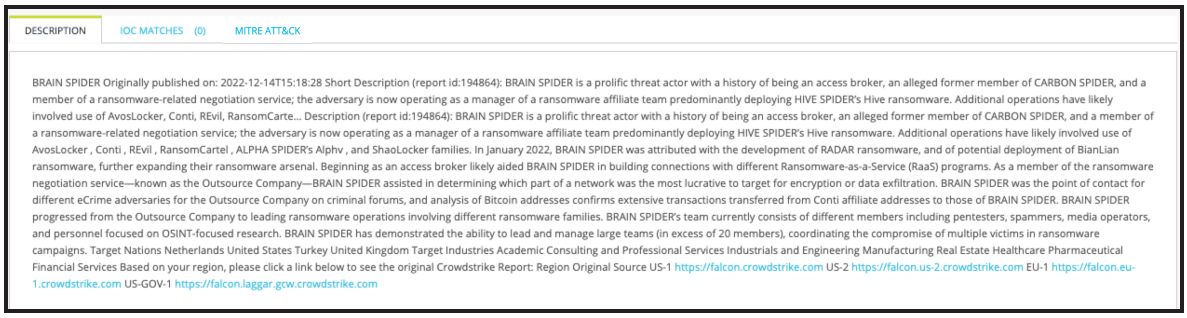
The following figure summarizes the Actor Details page sections.



1	Review key summary details. Click **Open in ThreatStream** to view the record in ThreatStream.
2	Total Match count.
3	Tags and other key details from ThreatStream.
4	Use the tabs to learn more: • **Description**: View the description from ThreatStream. See "Actor Description" on the next page. • **IOC Matches**: View an IOC Match results table. See "Matches" on the next page. • **MITRE ATT&CK**: View the MITRE technique matrix from ThreatStream. See "MITRE ATT&CK" on the next page.

Actor Description

The following figure shows the **Description** tab. The description is populated by the ThreatStream intel source.



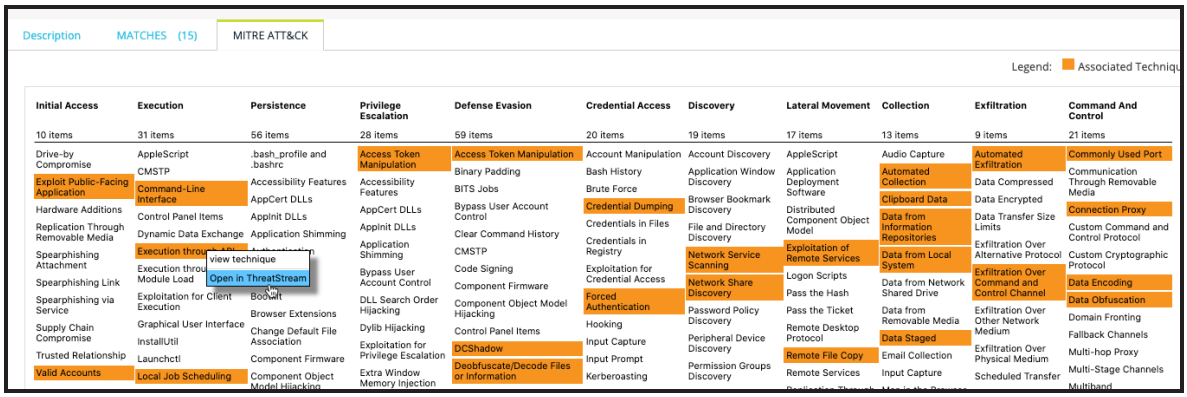
Matches

The details page has a tab for IOC matches.

The matches results tables can be used just like the IOC Match activity search results table. For details, see "IOC Match Results Table" on page 90.

MITRE ATT&CK

The following figure shows the **MITRE ATT&CK** tab. This tab identifies MITRE ATT&CK associations (if any). The intel for the MITRE ATT&CK matrix is maintained by your ThreatStream organization.



You can click an associated technique and select **view technique** or **Open in ThreatStream** to go to additional details hosted on attack.mitre.org or ThreatStream.

> **Note:** MITRE associations are based on your organization's MITRE release version setting in ThreatStream:
>
> - MITRE ATT&CK techniques associated with MITRE v6 and earlier are classified as *TTPs* in the Anomali Threat Model, and MITRE TTPs are used to identify associated attacks.
> - MITRE ATT&CK techniques and sub-techniques associated with MITRE v7 and later are classified as *attack patterns* in the Anomali Threat Model, and MITRE attack patterns are used to identify associated attacks.

Attack Pattern Activity Searches

Search the Attack Pattern index to examine attack pattern indicators that have matched event logs during the specified time period.

1	**Search text box**: Specify a keyword or field-based search expression. Keyword searches match any of the following fields: name, feed name, tags. Specify field-based name-value pairs for more precise targeting.
2	**Applied Filters**: Review and clear filters.
3	**ThreatStream Publication Timeline**: Bars indicate when the threat entity publication was last modified in ThreatStream. Click a bar to filter by date. Click and drag over two or more bars to set a date range filter.

About Attack Pattern Searches

The Anomali Threat Model is STIX-compatible and supports workflows for developing threat intelligence using a commonly understood taxonomy of threat entities. Security Analytics has a search index for the following threat model entities: Actors, Attack Patterns, Campaigns, TTPs, Threat Bulletins, and Vulnerabilities.

Attack Pattern refers to common methods of exploiting software reported by MITRE and other intelligence providers. You can perform searches based on details of Attack Patterns maintained by your organization in ThreatStream.

When you search the Threat Model index, you search by threat model entity fields. When you view a Security Analytics result details page, the record includes event log details for the match.

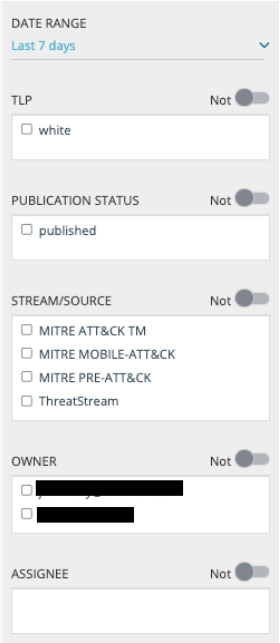
Note: MITRE associations are based on your organization's MITRE release version setting in ThreatStream:

- MITRE ATT&CK techniques associated with MITRE v6 and earlier are classified as *TTPs* in the Anomali Threat Model.
- MITRE ATT&CK techniques and sub-techniques associated with MITRE v7 and later are classified as *attack patterns* in the Anomali Threat Model.

Therefore, use the TTP search index if your ThreatStream organization uses MITRE v6 and earlier; use the Attack Pattern search index if your ThreatStream organization uses MITRE v7 and later.

Filter UI

You can use the filter UI to apply the following filters to your search:



- **Date Range**
  Select a time period, a relative expression, or a date range. The time period filter is based on the ThreatStream publication date (the timestamp for "Modified" in ThreatStream).
- **TLP**
  Select a TLP (Traffic Light Protocol) associated with the entity.
- **Publication Status**
  Select a publication status: New, Pending Review, Review Requested, Reviewed, or Published.
- **Stream/Source**
  Select the name of the Feed in ThreatStream.
- **Owner**
  Select the ThreatStream user who created the entity.
- **Assignee**
  Select the ThreatStream user assigned to investigate.

> **Note:** You can use negation in search expressions by selecting the **NOT** operator next to the filter heading. For example, to use negation with TLP, select the values you do not want to search and toggle on the **NOT** operator next to the TLP filter heading.

Filter Examples

```
modified_ts > "2021-11-09T15:50:00"
publication_status=new and tags=test
publication_status = published or publication_status = new
(publication_status != new) and (feed_name contains FD-5737 or FD-5989)
modified_ts > "2021-11-09T15:50:00" and (publication_status != new) and (feed_name contains FD-5737 or feed_name contains FD-5989)
tags = Reconnaissance or tags = "Command & Control (C2)"
tags in ['mitre-att&ck:detectable_by_common_defenses="Yes"', PRE-T1123] and (modified_ts < "2022-12-01")
```

Filter Operators

The following table describes the logical operators you can use to form complex field-based search expressions. Operator names are not case sensitive.

Field Type	Use this Operator
String	=, !=, contains, startswith, in (for lists) **Notes:** • The `startswith` operator matches any token in the field that starts with the pattern. For example, the expression `name startswith spider` matches a source field that has the value `GRACEFUL SPIDER`. • Use double quotes to escape special characters and spaces in searches with `=`, `!=`, and `in` operators. Examples: `name = "GRACEFUL SPIDER"`, `name != "GRACEFUL SPIDER"`, `tags in ["GENERAL_TTP:Bot", "ACTOR_TYPE:Nation State"]`
Numeric	=, !=, <, <=, >, >=, in (for lists) For example, `id in [312, 274]` **Note:** The `in` operator does not accept float and double types.
Date	=, !=, <, <=, >, >=
Logical	AND, OR, NOT, (*specify a parenthetical expression*)

Filter Fields

The following table describes all of the possible Attack Pattern search fields. The fields listed in the first column correspond with results table column names. The field names listed in the second column are the fields you specify when you form field-based name-value pair search expressions.

> **Note:** Not all fields are included as columns in the results table. When you search by fields without column names, you can locate the matching values in the details page. All of the fields listed in this table can be selected when you export results.

Column Name	Field Name	Type	Description
Assignee	assignee_user	String	User name on ThreatStream who is assigned to investigate.
Created	created_ts	Date	Timestamp of when the entity was created on ThreatStream. **Notes:** • In the results table, the time displayed is UTC time, adjusted for the browser time zone. • When you form search expressions, specify UTC time in the following format: <YYYY><MM><DD>T<HH>:<MM>:<SS>. The date part and the time part are separated by a capital T. You do not need to include T and the time values if you intend to search by date only. The following is an example of UTC time format: `2022-01-05T00:00:00` • You can also specify a time zone offset for searches where time zone precision is important. In the following example, the time zone offset is the `-08:00` at the end: `2022-01-05T00:00:00-08:00` • In exported results, the date and time are displayed as epoch time values. The following example shows the previous date-time example in epoch format: `1641342478`
Stream/Source	feed_name	String	Name of the feed in ThreatStream.

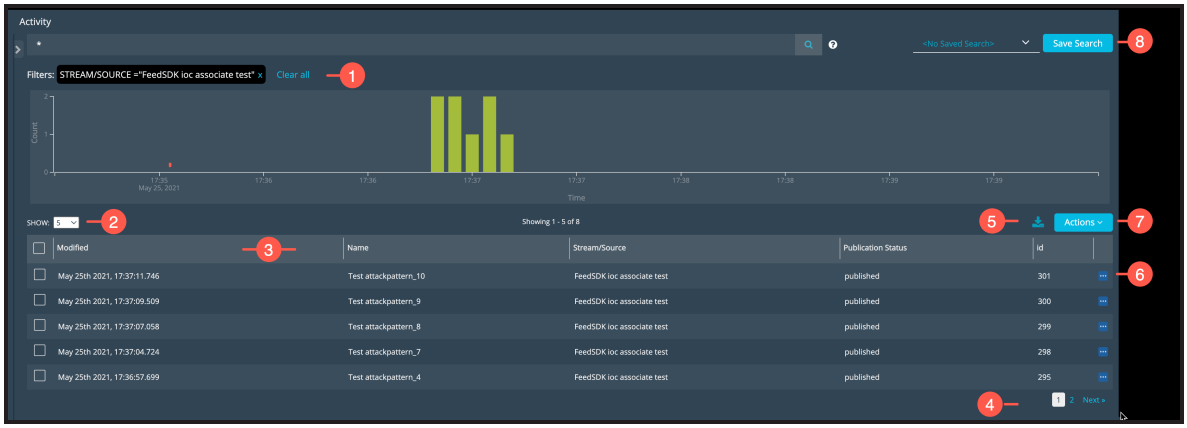
Column Name	Field Name	Type	Description
Modified	modified_ts	Date	Timestamp of when the entity was last updated on ThreatStream. **Notes:** • In the results table, the time displayed is UTC time, adjusted for the browser time zone. • When you form search expressions, specify UTC time in the following format: <YYYY><MM><DD>T<HH>:<MM>:<SS>. The date part and the time part are separated by a capital T. You do not need to include T and the time values if you intend to search by date only. The following is an example of UTC time format: `2022-01-05T00:00:00` • You can also specify a time zone offset for searches where time zone precision is important. In the following example, the time zone offset is the `-08:00` at the end: `2022-01-05T00:00:00-08:00` • In exported results, the date and time are displayed as epoch time values. The following example shows the previous date-time example in epoch format: `1641342478`
Name	name	String	Name of the entity.
Owner	owner_user	String	Name of the user in the organization on Anomali ThreatStream that created the entity.

Column Name	Field Name	Type	Description
Publication Status	publication_status	String	• `new` • `pending_review` • `review_requested` • `reviewed` • `published`
Published Date	published_ts	Date	Timestamp of when the entity was published on ThreatStream. **Notes:** • In the results table, the time displayed is UTC time, adjusted for the browser time zone. • When you form search expressions, specify UTC time in the following format: <YYYY><MM><DD>T<HH>:<MM>:<SS>. The date part and the time part are separated by a capital T. You do not need to include T and the time values if you intend to search by date only. The following is an example of UTC time format: `2022-01-05T00:00:00` • You can also specify a time zone offset for searches where time zone precision is important. In the following example, the time zone offset is the `-08:00` at the end: `2022-01-05T00:00:00-08:00` • In exported results, the date and time are displayed as epoch time values. The following example shows the previous date-time example in epoch format: `1641342478`

Column Name	Field Name	Type	Description
Tags	tags	String	Tags associated with the entity.
TLP	tlp	string	TLP (Traffic Light Protocol) color associated 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. Possible values: white, yellow, green, red

Attack Pattern Matches Results Table

The following figure identifies the UI elements that you use to manipulate the displayed results to find information about Attack Pattern matches.



1	Review and reset applied filters.
2	Select a number of rows per page.
3	Click the column header to sort the rows in ascending or descending order according to values in the column. Click a column header divider and drag it to make a column wider or more narrow.

4	Go to the next page of results or another page by page number.
5	Export the results table. See "Export Search Results" on page 66.
6	Display the Details page for the matched event. See "View Details" below.
7	Perform an action related to the selected row. See "Perform Actions" below.
8	Create a Saved Search configuration. See "Saved Searches" on page 65.

Perform Actions

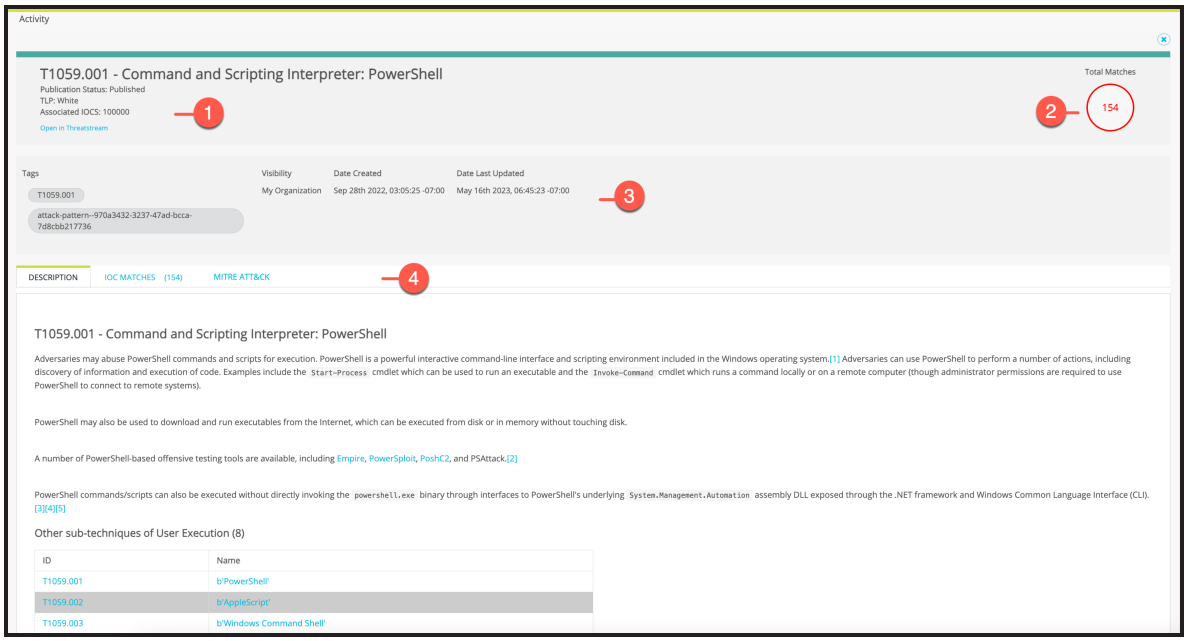
The Action menu above the results table allows you to perform the following actions.

Action	Description
Configure Fields	Select this option to configure the fields (columns) that appear in the results table.
Retrospective Search	Select this option to perform a retrospective search for the indicator correlated with the event.

View Details

···	Click the Details icon in the right-most column to display the details page.

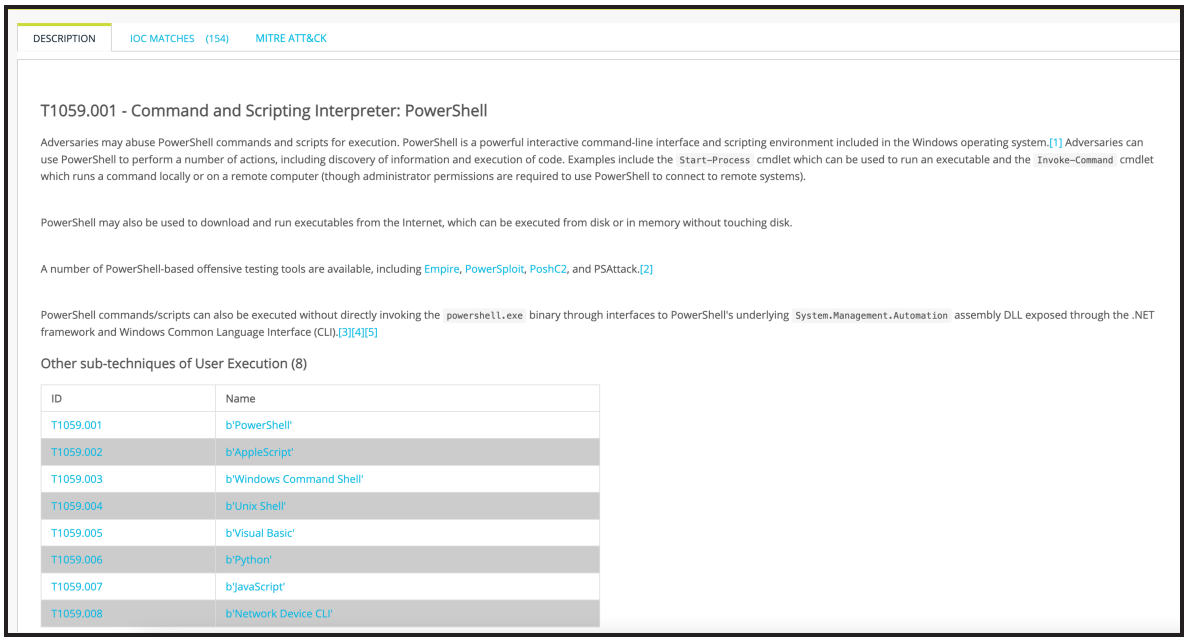
The following figure summarizes the Attack Pattern Details page sections.



1	Review key summary details. Click **Open in ThreatStream** to view the record in ThreatStream.
2	Total Match count.
3	Tags and other key details from ThreatStream.
4	Use the tabs to learn more: • **Description**: View the description from ThreatStream. See "Attack Pattern Description" below. • **IOC Matches**: View an IOC Match. See "Matches" on the next page.

Attack Pattern Description

The following figure shows the **Description** tab. The description is populated by the ThreatStream intel source.



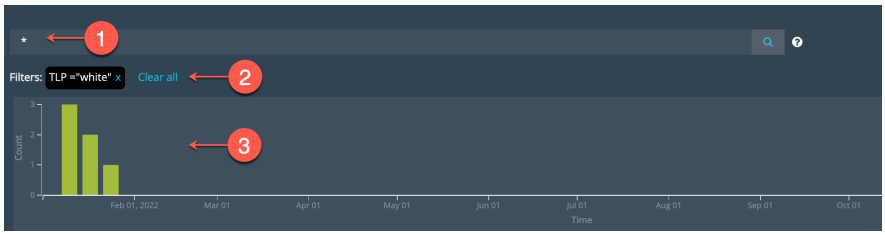
Matches

The details page has a tab for IOC matches.

The matches results tables can be used just like the IOC Match activity search results table. For details, see "IOC Match Results Table" on page 90.

Campaign Activity Searches

Search the Campaign index to examine threat campaigns provided by your threat intelligence feeds that have matched event logs during the specified time period.



1	**Search text box**: Specify a keyword or field-based search expression. Keyword searches match any of the following fields: name, feed name, tags. Specify field-based name-value pairs for more precise targeting.
2	**Applied Filters**: Review and clear filters.
3	**ThreatStream Publication Timeline**: Bars indicate when the threat entity publication was last modified in ThreatStream. Click a bar to filter by date. Click and drag over two or more bars to set a date range filter.

About Campaign Searches

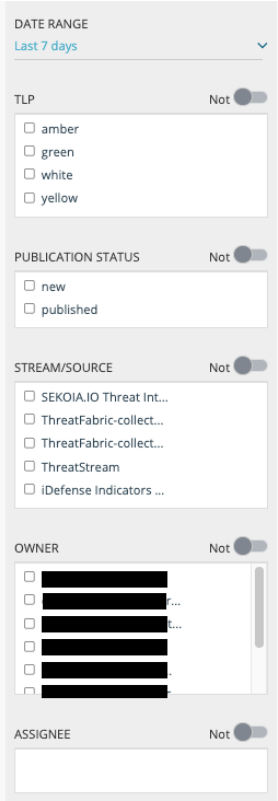
The Anomali Threat Model is STIX-compatible and supports workflows for developing threat intelligence using a commonly understood taxonomy of threat entities. Security Analytics has a search index for the following threat model entities: Actors, Attack Patterns, Campaigns, TTPs, Threat Bulletins, and Vulnerabilities.

A *Campaign* is a threat entity that refers to malicious activity orchestrated to achieve a common goal or to harm a specific target.

When you search the Threat Model index, you search by threat model entity fields. When you view a Security Analytics result details page, the record includes event log details for the match.

Filter UI

You can use the filter UI to apply the following filters to your search:


DATE RANGE
Last 7 days
TLP
Not
amber
green
white
yellow
PUBLICATION STATUS
Not
new
published
STREAM/SOURCE
Not
SEKOIA.IO Threat Int...
ThreatFabric-collect...
ThreatFabric-collect...
ThreatStream
iDefense Indicators ...
OWNER
Not
ASSIGNEE
Not

- **Date Range**
  Select a time period, a relative expression, or a date range. The time period filter is based on the ThreatStream publication date (the timestamp for "Modified" in ThreatStream).
- **TLP**
  Select a TLP (Traffic Light Protocol) associated with the entity.
- **Publication Status**
  Select a publication status: New, Pending Review, Review Requested, Reviewed, or Published.
- **Stream/Source**
  Select the name of the Feed in ThreatStream.
- **Owner**
  Select the ThreatStream user who created the entity.
- **Assignee**
  Select the ThreatStream user assigned to investigate.

> **Note:** You can use negation in search expressions by selecting the **NOT** operator next to the filter heading. For example, to use negation with TLP, select the values you do not want to search and toggle on the **NOT** operator next to the TLP filter heading.

Filter Examples

```
modified_ts > "2021-11-09T15:50:00"
```

```
publication_status=new and tags contains emot
```

```
feed_name contains sync or silo
```

```
(publication_status = published or new) and feed_name contains
silo
```

```
(publication_status != new) and (feed_name contains sync or silo)
```

```
modified_ts > "2021-11-09T15:50:00" and (publication_status !=
new) and (feed_name contains sync or silo)
```

```
tags in ["EMOTET-Trojan", "Sticky-Bandits"] and (modified_ts <
"2020-12-01")
```

Filter Operators

The following table describes the logical operators you can use to form complex field-based search expressions. Operator names are not case sensitive.

Field Type	Use this Operator
String	=, !=, contains, startswith, in (for lists) **Notes:** • The `startswith` operator matches any token in the field that starts with the pattern. For example, the expression `name startswith spider` matches a source field that has the value `GRACEFUL SPIDER`. • Use double quotes to escape special characters and spaces in searches with `=`, `!=`, and `in` operators. Examples: `name = "GRACEFUL SPIDER"`, `name != "GRACEFUL SPIDER"`, `tags in ["GENERAL_TTP:Bot", "ACTOR_TYPE:Nation State"]`
Numeric	=, !=, <, <=, >, >=, in (for lists) For example, `id in [312, 274]` **Note:** The `in` operator does not accept float and double types.
Date	=, !=, <, <=, >, >=
Logical	AND, OR, NOT, (*specify a parenthetical expression*)

Filter Fields

The following table describes all of the possible Campaign search fields. The fields listed in the first column correspond with results table column names. The field names listed in the second column are the fields you specify when you form field-based name-value pair search expressions.

> **Note:** Not all fields are included as columns in the results table. When you search by fields without column names, you can locate the matching values in the details page. All of the fields listed in this table can be selected when you export results.

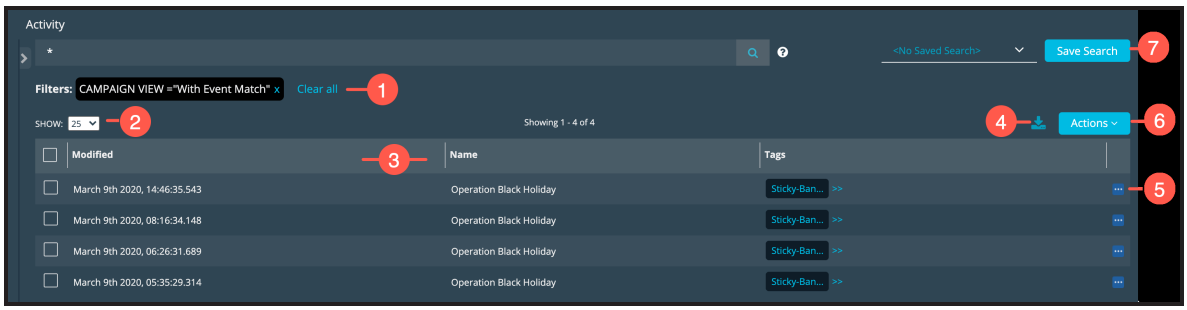
Column Name	Field Name	Type	Description
Assignee	assignee_user	String	User name on ThreatStream who is assigned to investigate.
Created	created_ts	Date	Timestamp of when the entity was created on ThreatStream. **Notes:** • In the results table, the time displayed is UTC time, adjusted for the browser time zone. • When you form search expressions, specify UTC time in the following format: <YYYY><MM><DD>T<HH>:<MM>:<SS>. The date part and the time part are separated by a capital T. You do not need to include T and the time values if you intend to search by date only. The following is an example of UTC time format: `2022-01-05T00:00:00` • You can also specify a time zone offset for searches where time zone precision is important. In the following example, the time zone offset is the `-08:00` at the end: `2022-01-05T00:00:00-08:00` • In exported results, the date and time are displayed as epoch time values. The following example shows the previous date-time example in epoch format: `1641342478`
Stream/Source	feed_name	String	Name of the feed in ThreatStream.

Column Name	Field Name	Type	Description
ID	id	Numeric	Entity ID in ThreatStream.
Modified	modified_ts	Date	Timestamp of when the entity was last updated on ThreatStream. **Notes:** • In the results table, the time displayed is UTC time, adjusted for the browser time zone. • When you form search expressions, specify UTC time in the following format: <YYYY><MM><DD>T<HH>:<MM>:<SS>. The date part and the time part are separated by a capital T. You do not need to include T and the time values if you intend to search by date only. The following is an example of UTC time format: `2022-01-05T00:00:00` • You can also specify a time zone offset for searches where time zone precision is important. In the following example, the time zone offset is the `-08:00` at the end: `2022-01-05T00:00:00-08:00` • In exported results, the date and time are displayed as epoch time values. The following example shows the previous date-time example in epoch format: `1641342478`
Name	name	String	Name of the entity.

Column Name	Field Name	Type	Description
Owner	owner_user	String	Name of the user in the organization on Anomali ThreatStream that created the entity.
Publication Status	publication_status	String	• `new` • `pending_review` • `review_requested` • `reviewed` • `published`
Tags	tags	String	Tags associated with the entity.
TLP	tlp	String	TLP (Traffic Light Protocol) color associated 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. Possible values: white, yellow, green, red

Campaign Matches Results Table

The following figure identifies the UI elements that you use to manipulate the displayed results to find information about Campaign matches.



1	Review and reset applied filters.
2	Select a number of rows per page.
3	Click the column header to sort the rows in ascending or descending order according to values in the column. Click a column header divider and drag it to make a column wider or more narrow.
4	Export the results table. See "Export Search Results" on page 66.
5	Display the Details page for the matched event. See "View Details" below.
6	Perform an action related to the selected row. See "Perform Actions" below.
7	Create a Saved Search configuration. See "Saved Searches" on page 65.

Perform Actions

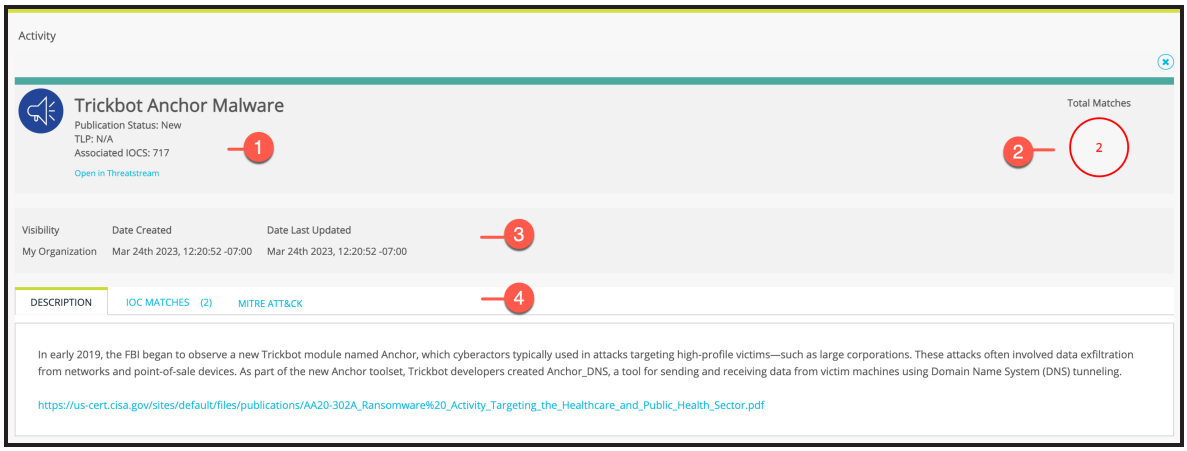
The Action menu above the results table allows you to perform the following actions.

Action	Description
Configure Fields	Select this option to configure the fields (columns) that appear in the results table.
Retrospective Search	Select this option to perform a retrospective search for the indicator correlated with the event.

View Details

•••	Click the Details icon in the right-most column to display the details page.

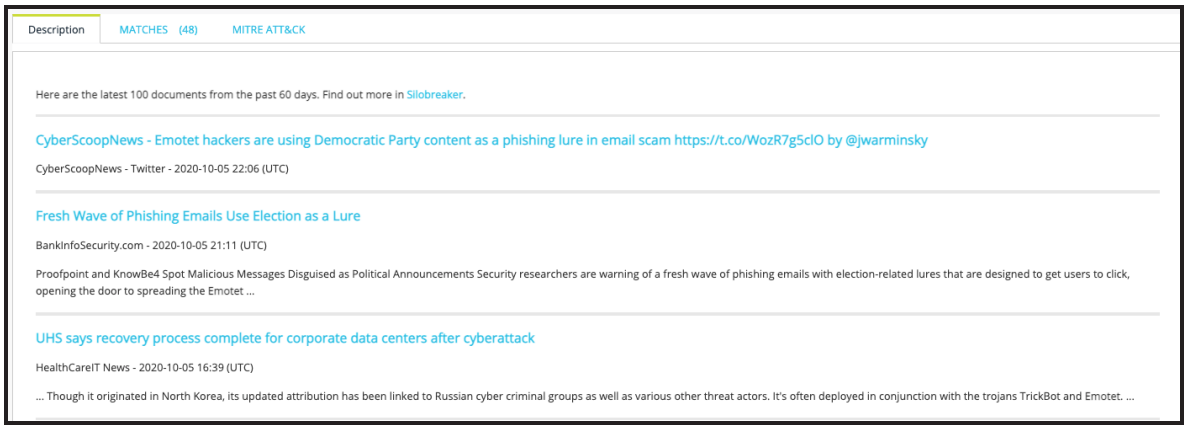
The following figure summarizes the Campaign Details page sections.



1	Review key summary details. Click **Open in ThreatStream** to view the record in ThreatStream.
2	Total Match count.
3	Tags and other key details from ThreatStream.
4	Use the tabs to learn more: • **Description**: View the description from ThreatStream. See "Campaign Description" below. • **IOC Matches**: View av IOC Match results table. See "Matches" on the next page. • **MITRE ATT&CK**: View the MITRE technique matrix from ThreatStream. See "MITRE ATT&CK" on the next page.

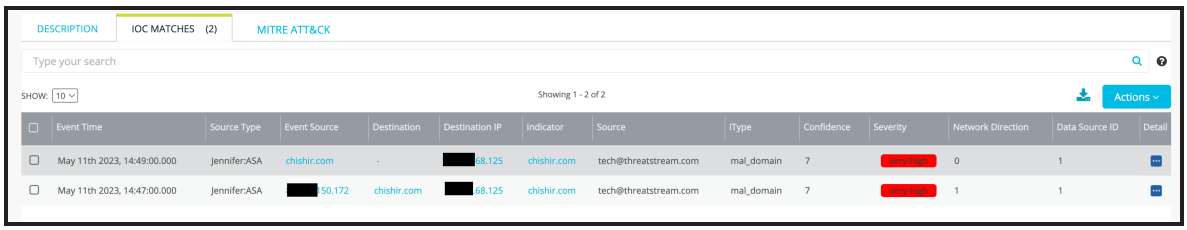
Campaign Description

The following figure shows the **Description** tab. The description is populated by the ThreatStream intel source.



Matches

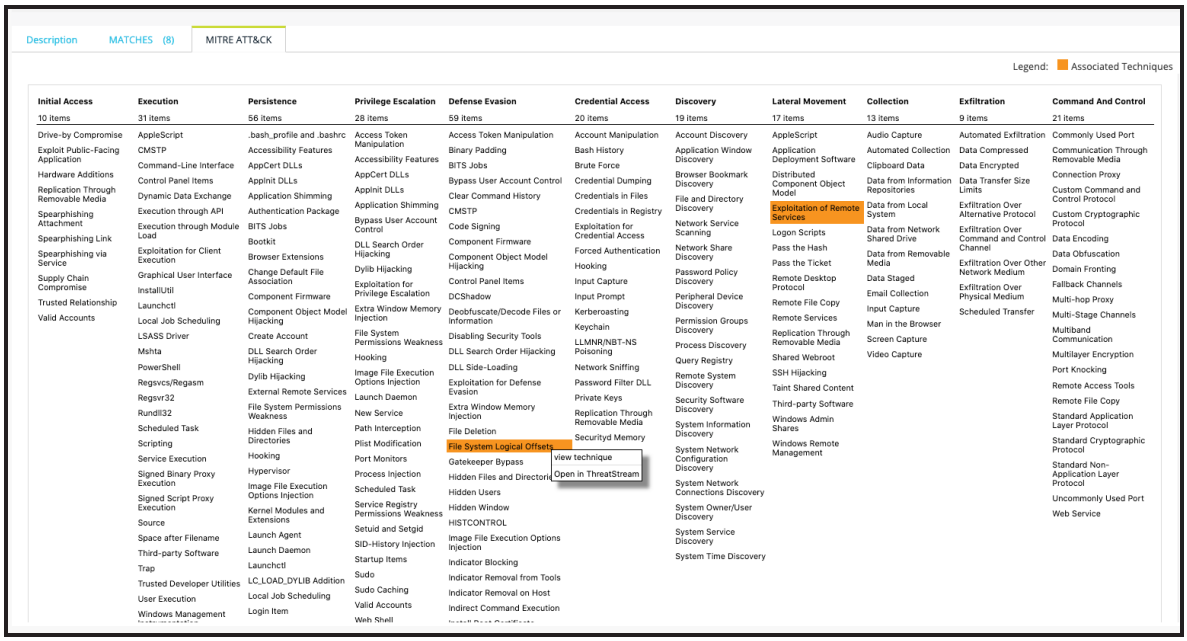
The details page has a tab for IOC matches.



The matches results tables can be used just like the IOC Match activity search results table. For details, see "IOC Match Results Table" on page 90.

MITRE ATT&CK

The following figure shows the **MITRE ATT&CK** tab. This tab identifies MITRE ATT&CK associations (if any). The intel for the MITRE ATT&CK matrix is maintained by your ThreatStream organization.

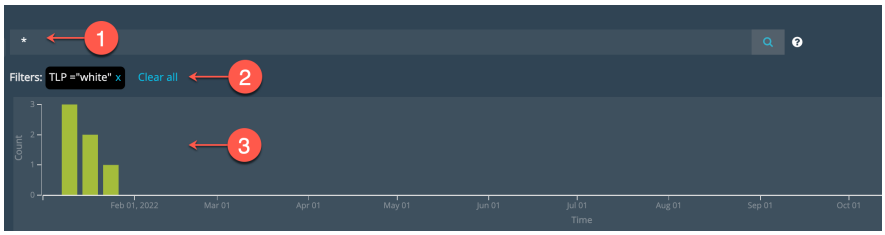


You can click an associated technique and select **view technique** or **Open in ThreatStream** to go to additional details hosted on attack.mitre.org or ThreatStream.

> **Note:** MITRE associations are based on your organization's MITRE release version setting in ThreatStream:
>
> - MITRE ATT&CK techniques associated with MITRE v6 and earlier are classified as *TTPs* in the Anomali Threat Model, and MITRE TTPs are used to identify associated attacks.
> - MITRE ATT&CK techniques and sub-techniques associated with MITRE v7 and later are classified as *attack patterns* in the Anomali Threat Model, and MITRE attack patterns are used to identify associated attacks.

Threat Bulletin Activity Searches

Search the Threat Bulletin index to examine Threat Bulletins provided by your threat intelligence feeds that have matched event logs during the specified time period.



1	**Search text box**: Specify a keyword or field-based search expression. Keyword searches match any of the following fields: name, feed name, tags. Specify field-based name-value pairs for more precise targeting.
2	**Applied Filters**: Review and clear filters.
3	**ThreatStream Publication Timeline**: Bars indicate when the threat entity publication was last modified in ThreatStream. Click a bar to filter by date. Click and drag over two or more bars to set a date range filter.

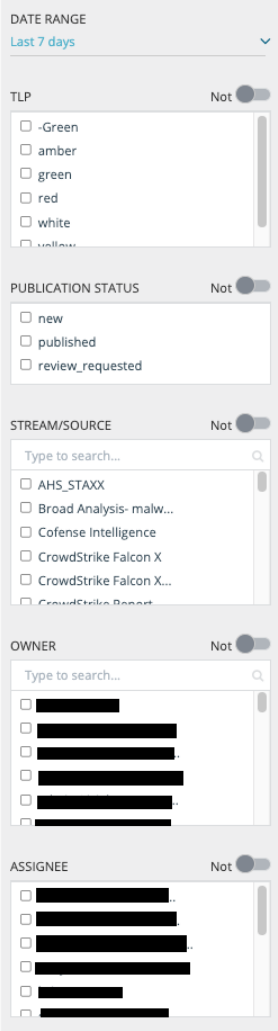
About Threat Bulletin Searches

The Anomali Threat Model is STIX-compatible and supports workflows for developing threat intelligence using a commonly understood taxonomy of threat entities. Security Analytics has a search index for the following threat model entities: Actors, Attack Patterns, Campaigns, TTPs, Threat Bulletins, and Vulnerabilities.

Threat Bulletins are news flashes, articles on Malware or attacker infrastructure, data dumps, and so on. Threat Bulletins 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.

When you search the Threat Model index, you search by threat model entity fields. When you view a Security Analytics result details page, the record includes event log details for the match.

Filter UI


DATE RANGE
Last 7 days
TLP
Not
-Green
amber
green
red
white
PUBLICATION STATUS
Not
new
published
review_requested
STREAM/SOURCE
Not
Type to search...
AHS_STAXX
Broad Analysis- malw...
Cofense Intelligence
CrowdStrike Falcon X
CrowdStrike Falcon X...
OWNER
Not
Type to search...
[redacted]
ASSIGNEE
Not
[redacted]

- **Date Range**
  Select a time period, a relative expression, or a date range. The time period filter is based on the ThreatStream publication date (the timestamp for "Modified" in ThreatStream).
- **TLP**
  Select a TLP (Traffic Light Protocol) associated with the entity.
- **Publication Status**
  Select a publication status: New, Pending Review, Review Requested, Reviewed, or Published.
- **Stream/Source**
  Select the name of the Feed in ThreatStream.
- **Owner**
  Select the ThreatStream user who created the entity.
- **Assignee**
  Select the ThreatStream user assigned to investigate.

> **Note:** You can use negation in search expressions by selecting the **NOT** operator next to the filter heading. For example, to use negation with TLP, select the values you do not want to search and toggle on the **NOT** operator next to the TLP filter heading.

Filter Examples

```
modified_ts > "2021-11-09T15:50:00"
```

```
publication_status=new and tags=test
```

```
(publication_status = published or new) and feed_name contains
misp
```

```
(publication_status != new) and (feed_name contains misp or group)
```

```
modified_ts > "2021-11-09T15:50:00" and (publication_status !=
new) and (feed_name contains misp or group)
```

```
tags in ["GIR:3.3", "admiralty-scale:information-credibility=1"]
and (modified_ts > "2020-12-01")
```

Filter Operators

The following table describes the logical operators you can use to form complex field-based search expressions. Operator names are not case sensitive.

Field Type	Use this Operator
String	=, !=, contains, startswith, in (for lists) **Notes:** • The `startswith` operator matches any token in the field that starts with the pattern. For example, the expression `name startswith spider` matches a source field that has the value `GRACEFUL SPIDER`. • Use double quotes to escape special characters and spaces in searches with `=`, `!=`, and `in` operators. Examples: `name = "GRACEFUL SPIDER"`, `name != "GRACEFUL SPIDER"`, `tags in ["GENERAL_TTP:Bot", "ACTOR_TYPE:Nation State"]`
Numeric	=, !=, <, <=, >, >=, in (for lists) For example, `id in [312, 274]` **Note:** The `in` operator does not accept float and double types.
Date	=, !=, <, <=, >, >=
Logical	AND, OR, NOT, (*specify a parenthetical expression*)

Filter Fields

The following table describes all of the possible Threat Bulletin search fields. The fields listed in the first column correspond with results table column names. The field names listed in the second column are the fields you specify when you form field-based name-value pair search expressions.

> **Note:** Not all fields are included as columns in the results table. When you search by fields without column names, you can locate the matching values in the details page. All of the fields listed in this table can be selected when you export results.

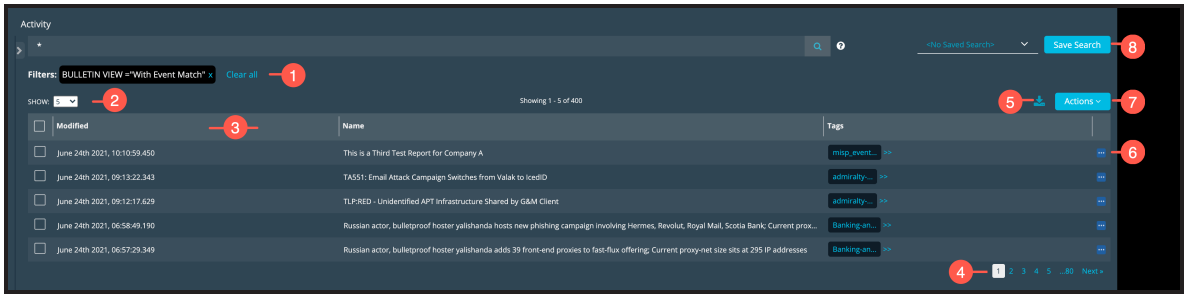
Column Name	Field Name	Type	Description
Assignee	assignee_user	String	User on ThreatStream to whom the Threat Bulletin is assigned for further investigation.
Created	created_ts	Date	Timestamp of when the entity was created on ThreatStream. **Notes:** • In the results table, the time displayed is UTC time, adjusted for the browser time zone. • When you form search expressions, specify UTC time in the following format: <YYYY><MM><DD>T<HH>:<MM>:<SS>. The date part and the time part are separated by a capital T. You do not need to include T and the time values if you intend to search by date only. The following is an example of UTC time format: `2022-01-05T00:00:00` • You can also specify a time zone offset for searches where time zone precision is important. In the following example, the time zone offset is the `-08:00` at the end: `2022-01-05T00:00:00-08:00` • In exported results, the date and time are displayed as epoch time values. The following example shows the previous date-time example in epoch format: `1641342478`
Stream/Source	feed_name	String	Name of the feed in ThreatStream.

Column Name	Field Name	Type	Description
ID	id	Numeric	Entity ID in ThreatStream.
Modified	modified_ts	Date	Timestamp of when the entity was last updated on ThreatStream. **Notes:** • In the results table, the time displayed is UTC time, adjusted for the browser time zone. • When you form search expressions, specify UTC time in the following format: <YYYY><MM><DD>T<HH>:<MM>:<SS>. The date part and the time part are separated by a capital T. You do not need to include T and the time values if you intend to search by date only. The following is an example of UTC time format: `2022-01-05T00:00:00` • You can also specify a time zone offset for searches where time zone precision is important. In the following example, the time zone offset is the `-08:00` at the end: `2022-01-05T00:00:00-08:00` • In exported results, the date and time are displayed as epoch time values. The following example shows the previous date-time example in epoch format: `1641342478`
Name	name	String	Name of the entity.
Owner	owner_user	String	ThreatStream user that created the entity.

Column Name	Field Name	Type	Description
Publication Status	publication_status	String	• `new` • `pending_review` • `review_requested` • `reviewed` • `published`
Tags	tags	String	Tags associated with the entity.
TLP	tlp	String	TLP (Traffic Light Protocol) color associated 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. Possible values: white, yellow, green, red

Threat Bulletin Matches Results Table

The following figure identifies the UI elements that you use to manipulate the displayed results to find information about Threat Bulletin matches.



1	Review and reset applied filters.

2	Select a number of rows per page.
3	Click the column header to sort the rows in ascending or descending order according to values in the column. Click a column header divider and drag it to make a column wider or more narrow.
4	Go to the next page of results or another page by page number.
5	Export the results table. See "Export Search Results" on page 66.
6	Display the Details page for the matched event. See "View Details" below.
7	Perform an action related to the selected row. See "Perform Actions" below.
8	Create a Saved Search configuration. See "Saved Searches" on page 65.

Perform Actions

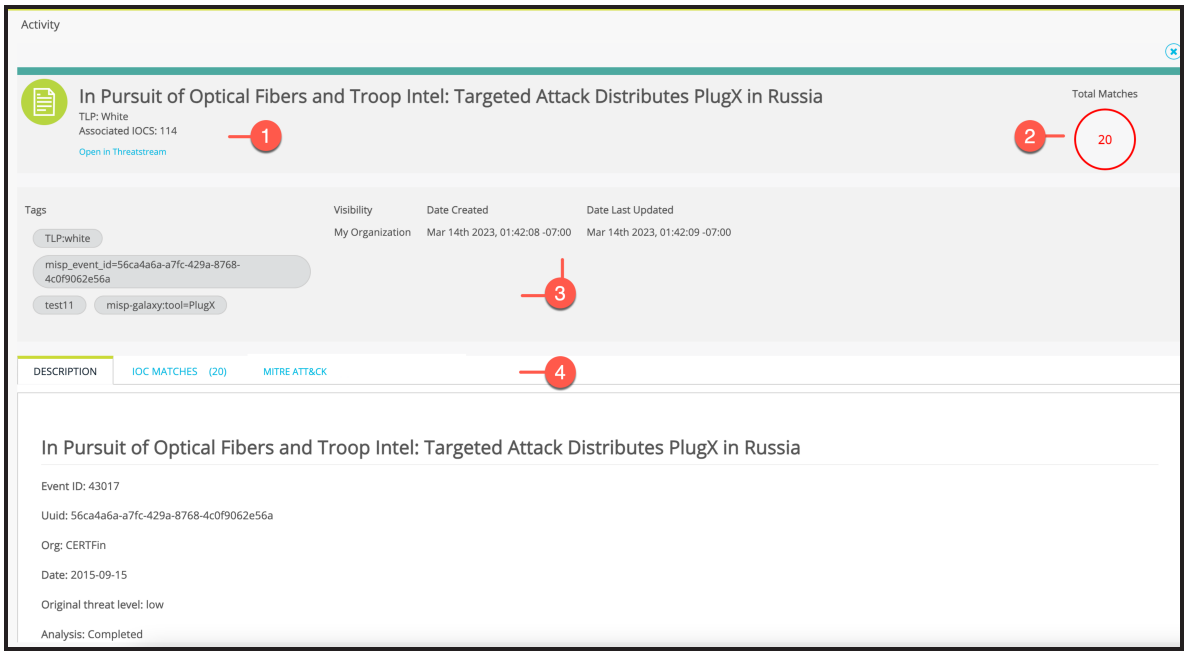
The Action menu above the results table allows you to perform the following actions.

Action	Description
Configure Fields	Select this option to configure the fields (columns) that appear in the results table.
Retrospective Search	Select this option to perform a retrospective search for the indicator correlated with the event.

View Details

···	Click the Details icon in the right-most column to display the details page.

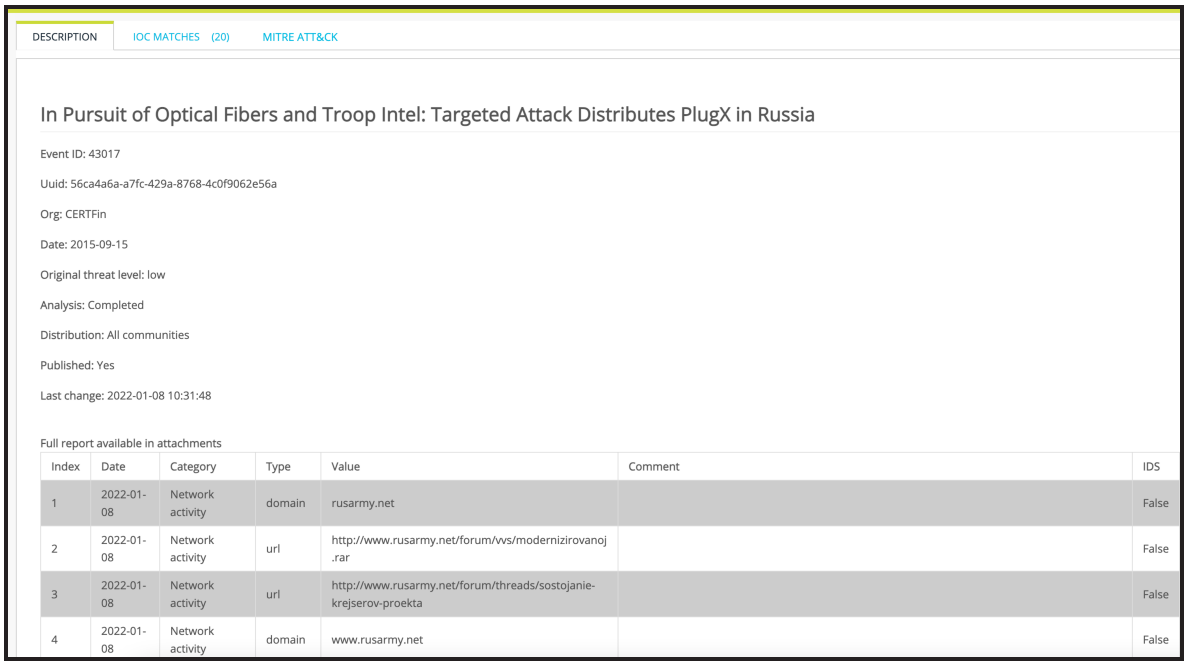
The following figure summarizes the Threat Bulletin Details page sections.



1	Review key summary details. Click **Open in ThreatStream** to view the record in ThreatStream.
2	Total Match count.
3	Tags and other key details from ThreatStream.
4	Use the tabs to learn more: • **Description**: View the description from ThreatStream. See "Threat Bulletin Description" below. • **IOC Matches**: View an IOC Match results table. See "Matches" on the next page. • **MITRE ATT&CK**: View the MITRE technique matrix from ThreatStream. See "MITRE ATT&CK" on the next page.

Threat Bulletin Description

The following figure shows the **Description** tab. The description is populated by the ThreatStream intel source.



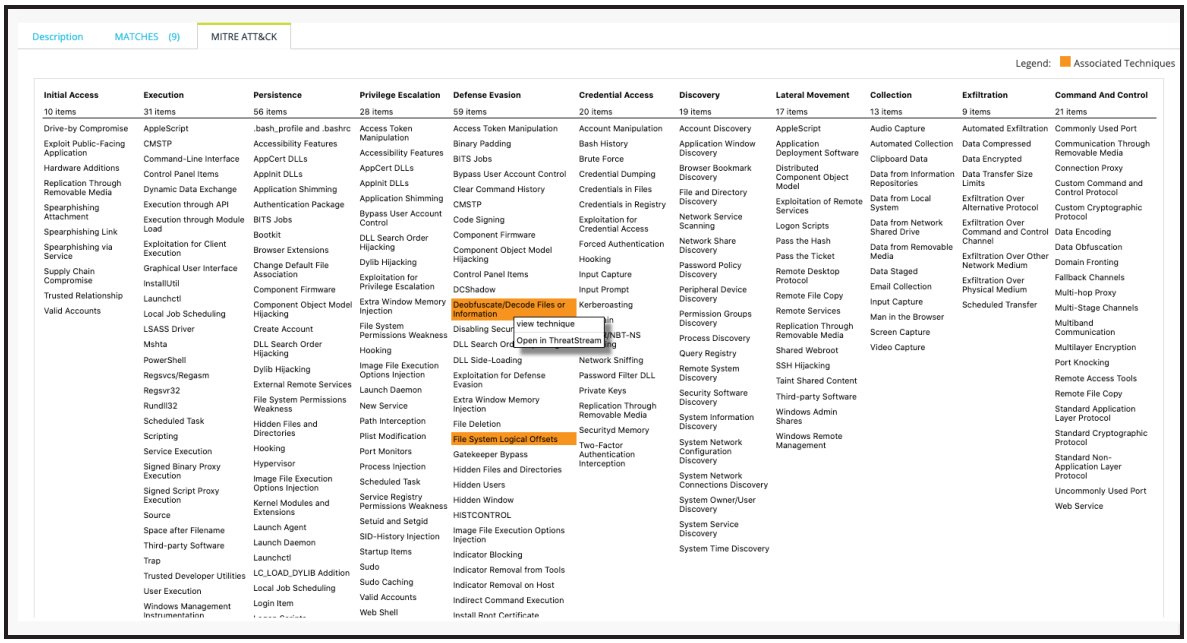
Matches

The details page has a tab for IOC matches.

The matches results tables can be used just like the IOC Match activity search results table. For details, see "IOC Match Results Table" on page 90.

MITRE ATT&CK

The following figure shows the **MITRE ATT&CK** tab. This tab identifies MITRE ATT&CK associations (if any). The intel for the MITRE ATT&CK matrix is maintained by your ThreatStream organization.

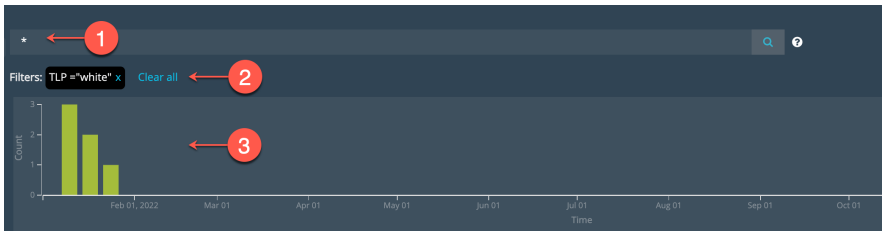


You can click an associated technique and select **view technique** or **Open in ThreatStream** to go to additional details hosted on attack.mitre.org or ThreatStream.

> **Note:** MITRE associations are based on your organization's MITRE release version setting in ThreatStream:
>
> - MITRE ATT&CK techniques associated with MITRE v6 and earlier are classified as *TTPs* in the Anomali Threat Model, and MITRE TTPs are used to identify associated attacks.
> - MITRE ATT&CK techniques and sub-techniques associated with MITRE v7 and later are classified as *attack patterns* in the Anomali Threat Model, and MITRE attack patterns are used to identify associated attacks.

TTP Activity Searches

Search the TTP index to examine MITRE ATT&CK TTP indicators that have matched event logs during the specified time period.



1	**Search text box**: Specify a keyword or field-based search expression. Keyword searches match any of the following fields: name, feed name, tags. Specify field-based name-value pairs for more precise targeting.
2	**Applied Filters**: Review and clear filters.
3	**ThreatStream Publication Timeline**: Bars indicate when the threat entity publication was last modified in ThreatStream. Click a bar to filter by date. Click and drag over two or more bars to set a date range filter.

About TTP Searches

The Anomali Threat Model is STIX-compatible and supports workflows for developing threat intelligence using a commonly understood taxonomy of threat entities. Security Analytics has a search index for the following threat model entities: Actors, Attack Patterns, Campaigns, TTPs, Threat Bulletins, and Vulnerabilities.

TTP refers to MITRE ATT&CK library of Tactics, Techniques, and Procedures (TTP) indicators. You can perform searches based on TTP details.

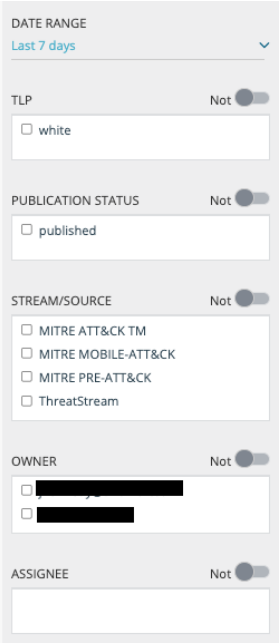
When you search the Threat Model index, you search by threat model entity fields. When you view a Security Analytics result details page, the record includes event log details for the match.

> **Note:** MITRE associations are based on your organization's MITRE release version setting in ThreatStream. MITRE ATT&CK techniques associated with MITRE v6 and earlier are classified as *TTPs* in the Anomali Threat Model. MITRE ATT&CK techniques and sub-techniques associated with MITRE v7 and later are classified as *attack patterns* in the Anomali Threat Model. Therefore, use the TTP search index if your ThreatStream organization uses MITRE v6 and earlier; use the Attack Pattern

search index if your ThreatStream organization uses MITRE v7 and later.

Filter UI

You can use the filter UI to apply the following filters to your search:



- **Date Range**
  Select a time period, a relative expression, or a date range. The time period filter is based on the ThreatStream publication date (the timestamp for "Modified" in ThreatStream).
- **TLP**
  Select a TLP (Traffic Light Protocol) associated with the entity.
- **Publication Status**
  Select a publication status: New, Pending Review, Review Requested, Reviewed, or Published.
- **Stream/Source**
  Select the name of the Feed in ThreatStream.
- **Owner**
  Select the ThreatStream user who created the entity.
- **Assignee**
  Select the ThreatStream user assigned to investigate.

> **Note:** You can use negation in search expressions by selecting the **NOT** operator next to the filter heading. For example, to use negation with TLP, select the values you do not want to search and toggle on the **NOT** operator next to the TLP filter heading.

Filter Examples

```
modified_ts > "2021-11-09T15:50:00"
publication_status=new and tags=test
publication_status = published or publication_status = new
(publication_status != new) and (feed_name contains FD-5737 or FD-5989)
modified_ts > "2021-11-09T15:50:00" and (publication_status != new) and (feed_name contains FD-5737 or feed_name contains FD-5989)
tags = Reconnaissance or tags = "Command & Control (C2)"
tags in ['mitre-att&ck:detectable_by_common_defenses="Yes"', PRE-T1123] and (modified_ts < "2022-12-01")
```

Filter Operators

The following table describes the logical operators you can use to form complex field-based search expressions. Operator names are not case sensitive.

Field Type	Use this Operator
String	=, !=, contains, startswith, in (for lists) **Notes:** • The `startswith` operator matches any token in the field that starts with the pattern. For example, the expression `name startswith spider` matches a source field that has the value `GRACEFUL SPIDER`. • Use double quotes to escape special characters and spaces in searches with `=`, `!=`, and `in` operators. Examples: `name = "GRACEFUL SPIDER"`, `name != "GRACEFUL SPIDER"`, `tags in ["GENERAL_TTP:Bot", "ACTOR_TYPE:Nation State"]`
Numeric	=, !=, <, <=, >, >=, in (for lists) For example, `id in [312, 274]` **Note:** The `in` operator does not accept float and double types.
Date	=, !=, <, <=, >, >=
Logical	AND, OR, NOT, (*specify a parenthetical expression*)

Filter Fields

The following table describes all of the possible TTP search fields. The fields listed in the first column correspond with results table column names. The field names listed in the second column are the fields you specify when you form field-based name-value pair search expressions.

> **Note:** Not all fields are included as columns in the results table. When you search by fields without column names, you can locate the matching values in the details page. All of the fields listed in this table can be selected when you export results.

Column Name	Field Name	Type	Description
Assignee	assignee_user	String	User name on ThreatStream who is assigned to investigate.
Created	created_ts	Date	Timestamp of when the entity was created on ThreatStream. **Notes:** • In the results table, the time displayed is UTC time, adjusted for the browser time zone. • When you form search expressions, specify UTC time in the following format: <YYYY><MM><DD>T<HH>:<MM>:<SS>. The date part and the time part are separated by a capital T. You do not need to include T and the time values if you intend to search by date only. The following is an example of UTC time format: `2022-01-05T00:00:00` • You can also specify a time zone offset for searches where time zone precision is important. In the following example, the time zone offset is the `-08:00` at the end: `2022-01-05T00:00:00-08:00` • In exported results, the date and time are displayed as epoch time values. The following example shows the previous date-time example in epoch format: `1641342478`
Stream/Source	feed_name	String	Name of the feed in ThreatStream.

Column Name	Field Name	Type	Description
Modified	modified_ts	Date	Timestamp of when the entity was last updated on ThreatStream. **Notes:** • In the results table, the time displayed is UTC time, adjusted for the browser time zone. • When you form search expressions, specify UTC time in the following format: <YYYY><MM><DD>T<HH>:<MM>:<SS>. The date part and the time part are separated by a capital T. You do not need to include T and the time values if you intend to search by date only. The following is an example of UTC time format: `2022-01-05T00:00:00` • You can also specify a time zone offset for searches where time zone precision is important. In the following example, the time zone offset is the `-08:00` at the end: `2022-01-05T00:00:00-08:00` • In exported results, the date and time are displayed as epoch time values. The following example shows the previous date-time example in epoch format: `1641342478`
Name	name	String	Name of the entity.
Owner	owner_user	String	Name of the user in the organization on Anomali ThreatStream that created the entity.

Column Name	Field Name	Type	Description
Publication Status	publication_status	String	• `new` • `pending_review` • `review_requested` • `reviewed` • `published`
Published Date	published_ts	Date	Timestamp of when the entity was published on ThreatStream. **Notes:** • In the results table, the time displayed is UTC time, adjusted for the browser time zone. • When you form search expressions, specify UTC time in the following format: <YYYY><MM><DD>T<HH>:<MM>:<SS>. The date part and the time part are separated by a capital T. You do not need to include T and the time values if you intend to search by date only. The following is an example of UTC time format: `2022-01-05T00:00:00` • You can also specify a time zone offset for searches where time zone precision is important. In the following example, the time zone offset is the `-08:00` at the end: `2022-01-05T00:00:00-08:00` • In exported results, the date and time are displayed as epoch time values. The following example shows the previous date-time example in epoch format: `1641342478`

Column Name	Field Name	Type	Description
Tags	tags	String	Tags associated with the entity.
TLP	tlp	string	TLP (Traffic Light Protocol) color associated 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. Possible values: white, yellow, green, red

TTP Matches Results Table

The following figure identifies the UI elements that you use to manipulate the displayed results to find information about TTP matches.

1	Review and reset applied filters.
2	Select a number of rows per page.
3	Click the column header to sort the rows in ascending or descending order according to values in the column. Click a column header divider and drag it to make a column wider or more narrow.
4	Go to the next page of results or another page by page number.
5	Export the results table. See "Export Search Results" on page 66.

6	Display the Details page for the matched event. See "View Details" below.
7	Perform an action related to the selected row. See "Perform Actions" below.
8	Create a Saved Search configuration. See "Saved Searches" on page 65.

Perform Actions

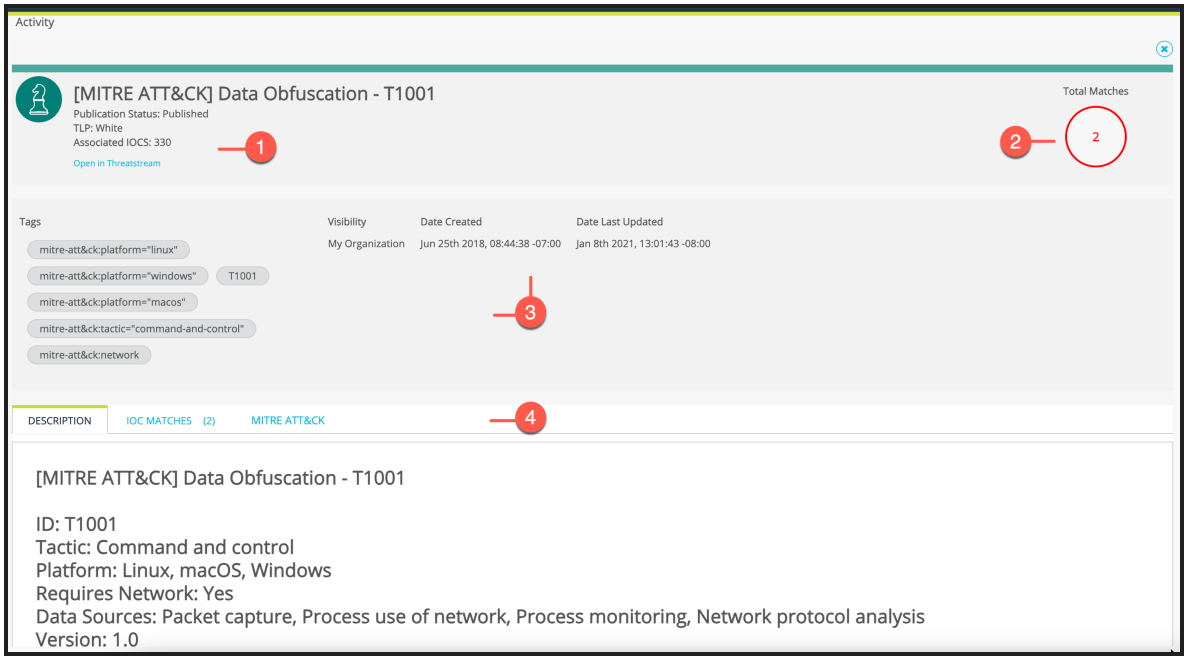
The Action menu above the results table allows you to perform the following actions.

Action	Description
Configure Fields	Select this option to configure the fields (columns) that appear in the results table.
Retrospective Search	Select this option to perform a retrospective search for the indicator correlated with the event.

View Details

•••	Click the Details icon in the right-most column to display the details page.

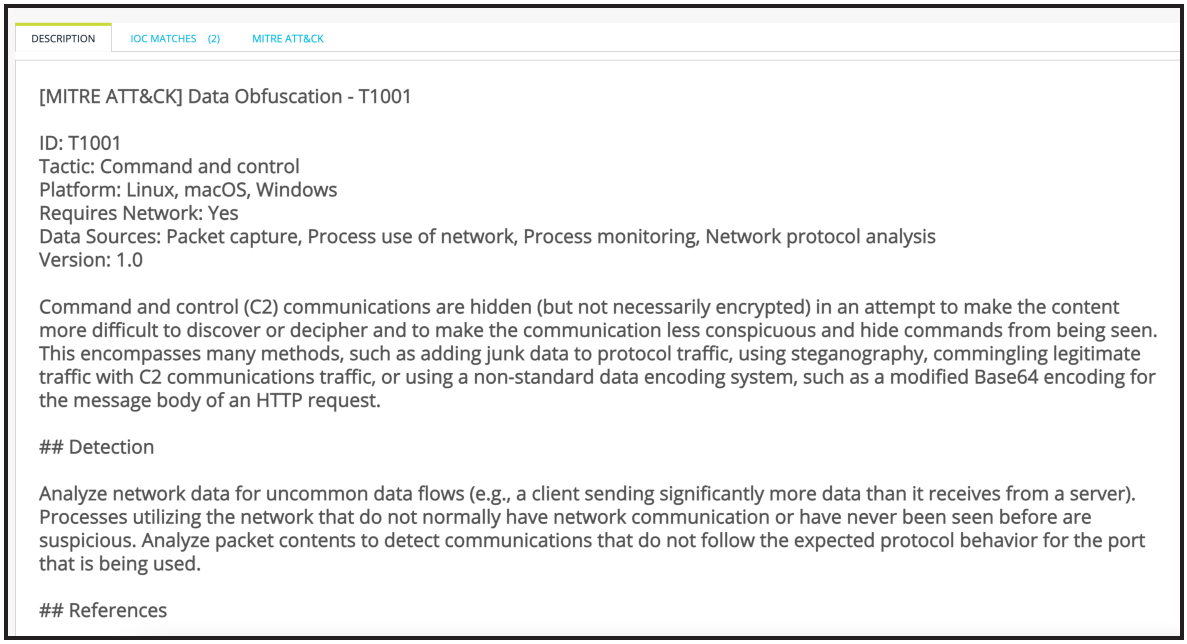
The following figure summarizes the TTP Details page sections.



1	Review key summary details. Click **Open in ThreatStream** to view the record in ThreatStream.
2	Total Match count.
3	Tags and other key details from ThreatStream.
4	Use the tabs to learn more: • **Description**: View the description from ThreatStream. See "TTP Description" below. • **IOC Matches**: View an IOC Match results table. See "Matches" below. • **MITRE ATT&CK**: View the MITRE technique matrix from ThreatStream. See "MITRE ATT&CK" on the next page.

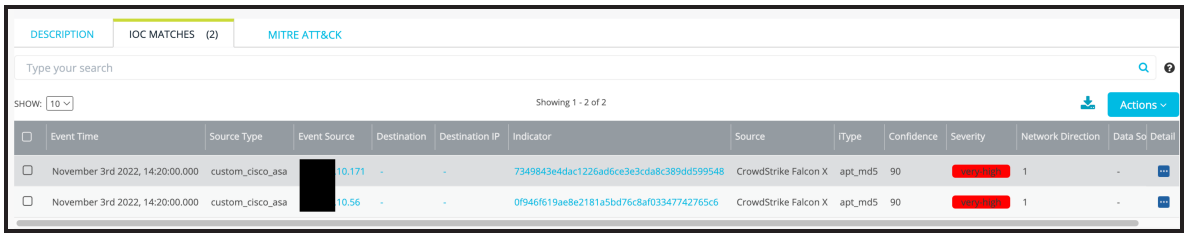
TTP Description

The following figure shows the **Description** tab. The description is populated by the ThreatStream intel source.



Matches

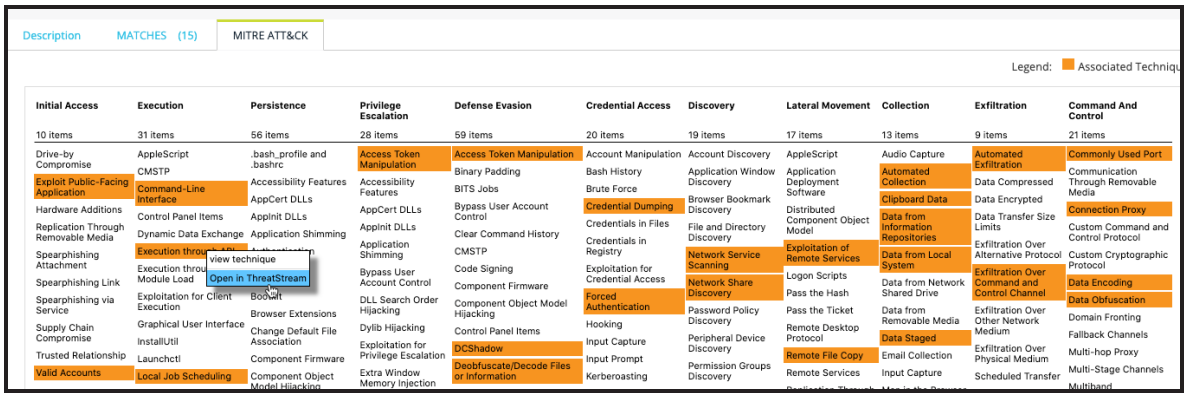
The details page has a tab for IOC matches.



The matches results tables can be used just like the IOC Match activity search results table. For details, see "IOC Match Results Table" on page 90.

MITRE ATT&CK

The following figure shows the **MITRE ATT&CK** tab. This tab identifies MITRE ATT&CK associations (if any). The intel for the MITRE ATT&CK matrix is maintained by your ThreatStream organization.



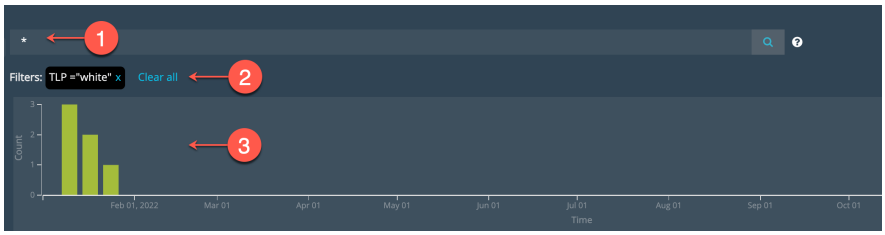
You can click an associated technique and select **view technique** or **Open in ThreatStream** to go to additional details hosted on attack.mitre.org or ThreatStream.

Note: MITRE associations are based on your organization's MITRE release version setting in ThreatStream:

- MITRE ATT&CK techniques associated with MITRE v6 and earlier are classified as *TTPs* in the Anomali Threat Model, and MITRE TTPs are used to identify associated attacks.
- MITRE ATT&CK techniques and sub-techniques associated with MITRE v7 and later are classified as *attack patterns* in the Anomali Threat Model, and MITRE attack patterns are used to identify associated attacks.

Vulnerability Activity Searches

Search the Vulnerability index to examine Vulnerabilities provided by your threat intelligence feeds that have matched event logs during the specified time period.



1	**Search text box**: Specify a keyword or field-based search expression. Keyword searches match any of the following fields: name, feed name, tags. Specify field-based name-value pairs for more precise targeting.
2	**Applied Filters**: Review and clear filters.
3	**ThreatStream Publication Timeline**: Bars indicate when the threat entity publication was last modified in ThreatStream. Click a bar to filter by date. Click and drag over two or more bars to set a date range filter.

About Vulnerability Searches

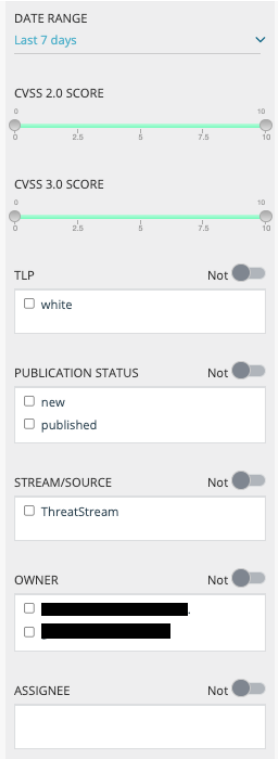
The Anomali Threat Model is STIX-compatible and supports workflows for developing threat intelligence using a commonly understood taxonomy of threat entities. Security Analytics has a search index for the following threat model entities: Actors, Attack Patterns, Campaigns, TTPs, Threat Bulletins, and Vulnerabilities.

Anomali ThreatStream imports a large number of Vulnerabilities from outside sources, such as the National Vulnerability Database (https://nvd.nist.gov/vuln/data-feeds), on a daily basis. You can perform searches based on Vulnerability details, such as Common Vulnerability Scoring System (CVSS) score.

When you search the Threat Model index, you search by threat model entity fields. When you view a Security Analytics result details page, the record includes event log details for the match.

Filter UI

You can use the filter UI to apply the following filters to your search:


DATE RANGE
Last 7 days
CVSS 2.0 SCORE
CVSS 3.0 SCORE
TLP
Not
white
PUBLICATION STATUS
Not
new
published
STREAM/SOURCE
Not
ThreatStream
OWNER
Not
[redacted]
[redacted]
ASSIGNEE
Not

- **Date Range**
  Select a time period, a relative expression, or a date range. The time period filter is based on the ThreatStream publication date (the timestamp for "Modified" in ThreatStream).
- **CVSS 2.0 Score**
  CVSS score according to the CVSS 2.0 specification.
- **CVSS 3.0 Score**
  CVSS score according to the CVSS 3.0 specification.
- **TLP**
  Select a TLP (Traffic Light Protocol) associated with the entity.
- **Publication Status**
  Select a publication status: New, Pending Review, Review Requested, Reviewed, or Published.
- **Stream/Source**
  Select the name of the Feed in ThreatStream.
- **Owner**
  Select the ThreatStream user who created the entity.
- **Assignee**
  Select the ThreatStream user assigned to investigate.

> **Note:** You can use negation in search expressions by selecting the **NOT** operator next to the filter heading. For example, to use negation with TLP, select the values you do not want to search and toggle on the **NOT** operator next to the TLP filter heading.

Filter Examples

```
modified_ts > "2021-11-09T15:50:00"
```

```
cvss2_score > 7
```

```
publication_status=published and cvss2_score > 7
```

```
(publication_status = published or new) and feed_name contains
silo
```

```
(publication_status != new) and (feed_name contains silo or crowd)
```

```
modified_ts > "2021-11-09T15:50:00" and (publication_status !=
new) and (feed_name contains silo or crowd)
```

```
tags in ["NVD-CWE-noinfo", "CWE-416"] and (modified_ts > "2018-12-
01")
```

Filter Operators

The following table describes the logical operators you can use to form complex field-based search expressions. Operator names are not case sensitive.

Field Type	Use this Operator
String	=, !=, contains, startswith, in (for lists) **Notes:** • The `startswith` operator matches any token in the field that starts with the pattern. For example, the expression `name startswith spider` matches a source field that has the value `GRACEFUL SPIDER`. • Use double quotes to escape special characters and spaces in searches with `=`, `!=`, and `in` operators. Examples: `name = "GRACEFUL SPIDER"`, `name != "GRACEFUL SPIDER"`, `tags in ["GENERAL_TTP:Bot", "ACTOR_TYPE:Nation State"]`
Numeric	=, !=, <, <=, >, >=, in (for lists) For example, `id in [312, 274]` **Note:** The `in` operator does not accept float and double types.
Date	=, !=, <, <=, >, >=
Logical	AND, OR, NOT, (*specify a parenthetical expression*)

Filter Fields

The following table describes all of the possible Vulnerability search fields. The fields listed in the first column correspond with results table column names. The field names listed in the second column are the fields you specify when you form field-based name-value pair search expressions.

> **Note:** Not all fields are included as columns in the results table. When you search by fields without column names, you can locate the matching values in the details page. All of the fields listed in this table can be selected when you export results.

Column Name	Field Name	Type	Description
Assignee	assignee_user	String	User on ThreatStream to whom the vulnerability is assigned for further investigation.
Created	created_ts	Date	Timestamp of when the entity was created on ThreatStream. **Notes:** • In the results table, the time displayed is UTC time, adjusted for the browser time zone. • When you form search expressions, specify UTC time in the following format: <YYYY><MM><DD>T<HH>:<MM>:<SS>. The date part and the time part are separated by a capital T. You do not need to include T and the time values if you intend to search by date only. The following is an example of UTC time format: `2022-01-05T00:00:00` • You can also specify a time zone offset for searches where time zone precision is important. In the following example, the time zone offset is the `-08:00` at the end: `2022-01-05T00:00:00-08:00` • In exported results, the date and time are displayed as epoch time values. The following example shows the previous date-time example in epoch format: `1641342478`
CVSS 2.0 Score	cvss2_score	Numeric	CVSS score according to the CVSS 2.0 specification.

Column Name	Field Name	Type	Description
CVSS 3.0 Score	cvss3_score	Numeric	CVSS score according to the CVSS 3.0 specification.
Stream/Source	feed_name	String	Name of the feed in ThreatStream.
ID	id	Numeric	Entity ID in ThreatStream.

Column Name	Field Name	Type	Description
Modified	modified_ts	Date	Timestamp of when the entity was last updated on ThreatStream. **Notes:** • In the results table, the time displayed is UTC time, adjusted for the browser time zone. • When you form search expressions, specify UTC time in the following format: <YYYY><MM><DD>T<HH>:<MM>:<SS>. The date part and the time part are separated by a capital T. You do not need to include T and the time values if you intend to search by date only. The following is an example of UTC time format: `2022-01-05T00:00:00` • You can also specify a time zone offset for searches where time zone precision is important. In the following example, the time zone offset is the `-08:00` at the end: `2022-01-05T00:00:00-08:00` • In exported results, the date and time are displayed as epoch time values. The following example shows the previous date-time example in epoch format: `1641342478`
Name	name	String	Name of the entity. The names of Vulnerabilities are CVE numbers. Example: CVE-2018-20250

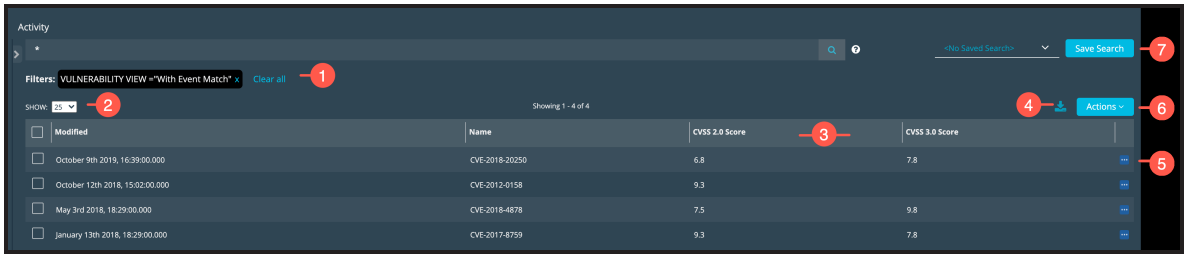
Column Name	Field Name	Type	Description
Owner	owner_user	String	Name of the user in the organization on ThreatStream that created the entity.
Publication Status	publication_status	String	• `new` • `pending_review` • `review_requested` • `reviewed` • `published`

Column Name	Field Name	Type	Description
Published	published_ts	date	Timestamp of when the entity was published on ThreatStream. **Notes:** • In the results table, the time displayed is UTC time, adjusted for the browser time zone. • When you form search expressions, specify UTC time in the following format: <YYYY><MM><DD>T<HH>:<MM>:<SS>. The date part and the time part are separated by a capital T. You do not need to include T and the time values if you intend to search by date only. The following is an example of UTC time format: `2022-01-05T00:00:00` • You can also specify a time zone offset for searches where time zone precision is important. In the following example, the time zone offset is the `-08:00` at the end: `2022-01-05T00:00:00-08:00` • In exported results, the date and time are displayed as epoch time values. The following example shows the previous date-time example in epoch format: `1641342478`
Tags	tags	String	Tags associated with the entity.

Column Name	Field Name	Type	Description
TLP	tlp	String	TLP (Traffic Light Protocol) color associated 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. Possible values: white, yellow, green, red

Vulnerability Matches Results Table

The following figure identifies the UI elements that you use to manipulate the displayed results to find information about Vulnerability matches.



1	Review and reset applied filters.
2	Select a number of rows per page.
3	Click the column header to sort the rows in ascending or descending order according to values in the column. Click a column header divider and drag it to make a column wider or more narrow.
4	Export the results table. See "Export Search Results" on page 66.
5	Display the Details page for the matched event. See "View Details" on the next page.

6	Perform an action related to the selected row. See "Perform Actions" below.
7	Create a Saved Search configuration. See "Saved Searches" on page 65.

Perform Actions

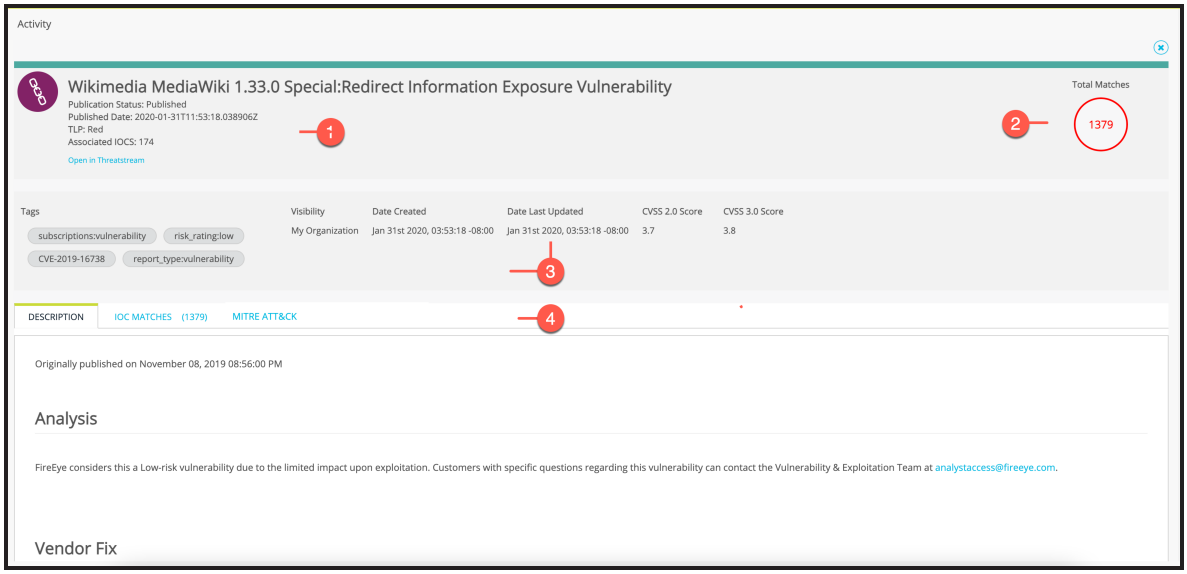
The Action menu above the results table allows you to perform the following actions.

Action	Description
Configure Fields	Select this option to configure the fields (columns) that appear in the results table.
Retrospective Search	Select this option to perform a retrospective search for the indicator correlated with the event.

View Details

•••	Click the Details icon in the right-most column to display the details page.

The following figure summarizes the Vulnerability Details page sections.

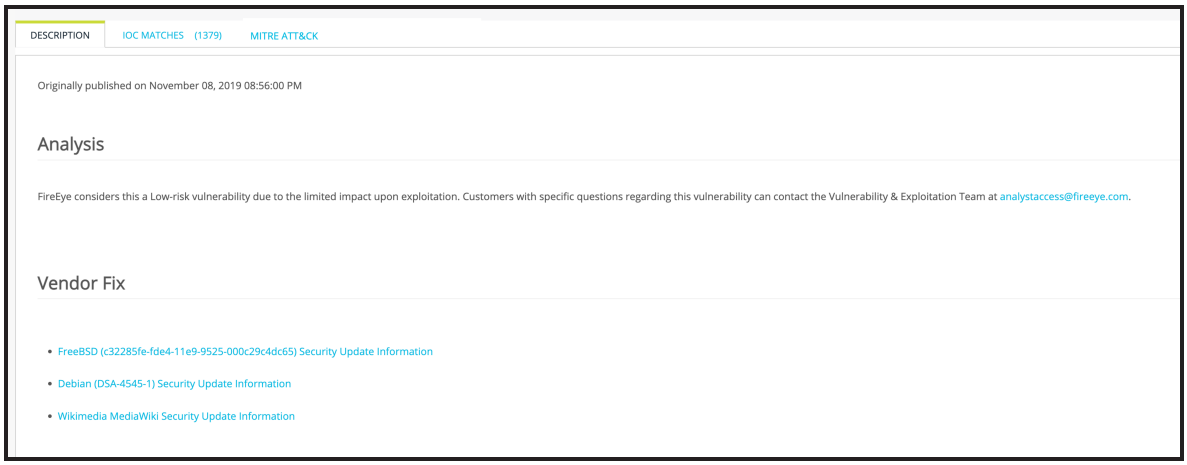


1	Review key summary details. Click **Open in ThreatStream** to view the record in ThreatStream.

2	Total Match count.
3	Tags and other key details from ThreatStream.
4	Use the tabs to learn more: • **Description**: View the description from ThreatStream. See "Vulnerability Description" below. • **IOC Matches**: View an IOC Match results table. See "Matches" below. • **MITRE ATT&CK**: View the MITRE technique matrix from ThreatStream. See "Vulnerability Activity Searches" on page 167.

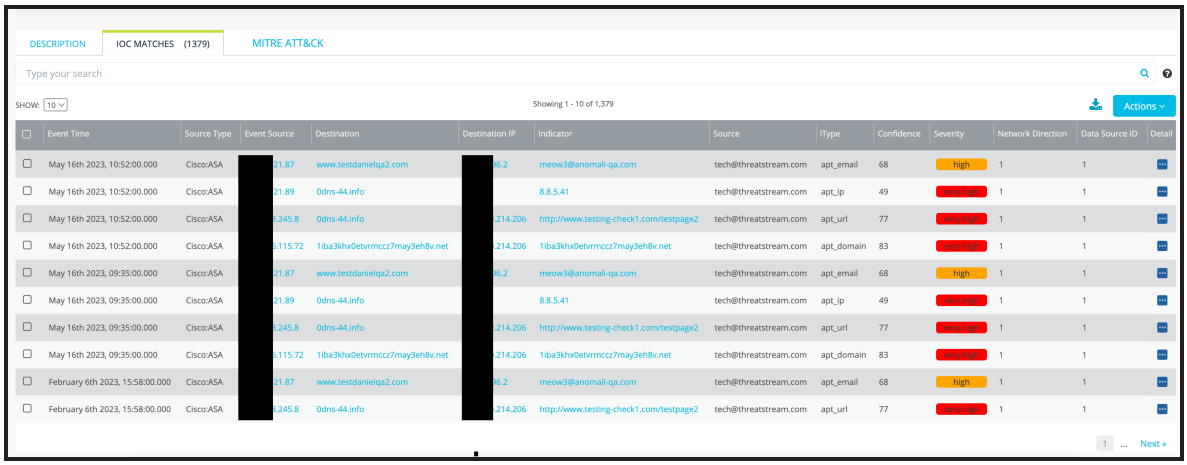
Vulnerability Description

The following figure shows the **Description** tab. The description is populated by the ThreatStream intel source.



Matches

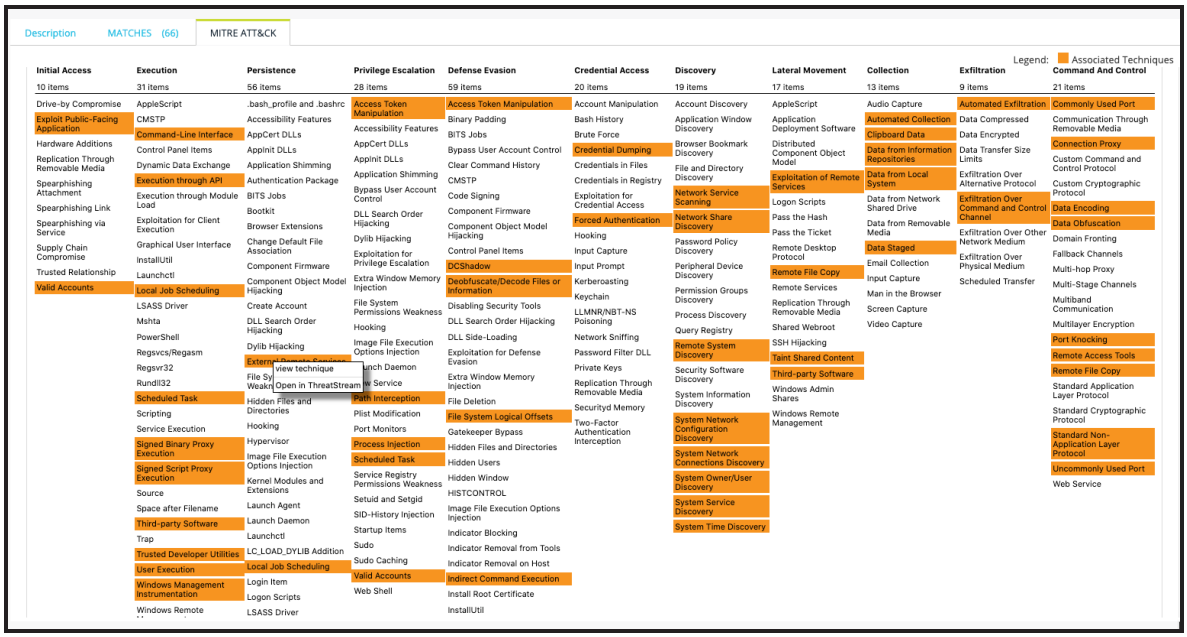
The details page has a tab for IOC matches.



The matches results tables can be used just like the IOC Match activity search results table. For details, see "IOC Match Results Table" on page 90.

MITRE ATT&CK

The following figure shows the **MITRE ATT&CK** tab. This tab identifies MITRE ATT&CK associations (if any). The intel for the MITRE ATT&CK matrix is maintained by your ThreatStream organization.

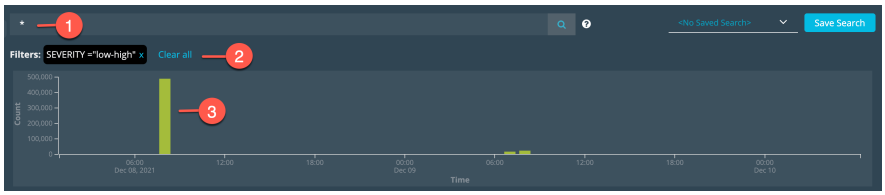


You can click an associated technique and select **view technique** or **Open in ThreatStream** to go to additional details hosted on attack.mitre.org or ThreatStream.

> **Note:** MITRE associations are based on your organization's MITRE release version setting in ThreatStream:
>
> - MITRE ATT&CK techniques associated with MITRE v6 and earlier are classified as *TTPs* in the Anomali Threat Model.
> - MITRE ATT&CK techniques and sub-techniques associated with MITRE v7 and later are classified as *attack patterns* in the Anomali Threat Model, and MITRE attack patterns are used to identify associated attacks. If your MITRE version is v7 or later, this tab may show MITRE attack patterns.

Alerts Activity Searches

Search the Alerts index to examine alerts that match your search terms during the specified time period.



1	**Search text box**: Specify a keyword or field-based search expression. Keyword searches match any field. Specify field-based name-value pairs for more precise targeting.
2	**Applied Filters**: Review and clear filters.
3	**Alerts Timeline**: Click a bar to filter by date. Click and drag over two or more bars to set a date range filter.

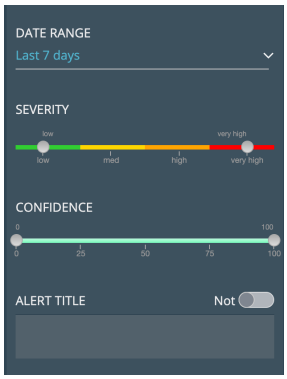
About Alerts Searches

The Alerts index is populated by alerts rules having the **List on Activity Page** action.

When you search the Alerts index, you search by alert fields. When you view a Security Analytics result details page, the record includes event log details for the match.

Filter UI

You can use the filter UI to apply the following filters to your search:



- **Date Range**
  Select a time period, a relative expression, or a date range. The time period filter is based on alert time; in other words, the timestamp when the alert was triggered.

- **Severity**
  Use the slider to specify an event severity range or drag both ends of the slider to a single severity to filter on just one. Event severity is determined by the indicator that matched the event log.

- **Confidence**
  Use the slider to specify a confidence score range. Confidence score indicates the certainty that an observable exhibits or is connected to malicious behavior. Confidence score is set by a ThreatStream machine learning algorithm that takes many factors into account, but can be overridden by analysts.

- **Alert Title**
  Select a title. The title field is populated by the rule configuration name.

> **Note:** You can use negation in search expressions by selecting the **NOT** operator next to the filter heading. For example, to use negation with Alert Title, select the titles you do not want to search and toggle on the **NOT** operator next to the Alert Title heading.

Filter Examples

```
indicator contains .com
severity = (high or very-high)
```

```
itype in ["mal_url", "mal_domain"]
alert_time >= 2021-12-10T19:18:51.062760Z
match_description contains "no event was received"
match_description contains restored
```

Filter Operators

The following table describes the logical operators you can use to form complex field-based search expressions. Operator names are **not** case sensitive.

Field Type	Use this Operator
String	=, !=, contains, startswith, in (for lists) **Note:** • The `startswith` operator matches any token in the field that starts with the pattern. For example, the expression `rule_name startswith critical` matches a source field that has the value `New Threats Against Critical Targets`. • Use double quotes to escape special characters and spaces in searches with `=`, `!=`, and `in` operators. For example, `itype in ["mal_url", "mal_domain"]`
Numeric	=, !=, <, <=, >, >=, in (for lists) For example, `confidence in [80, 90]` **Note:** The `in` operator does not accept float and double types.
Date	=, !=, <, <=, >, >=
Logical	AND, OR, NOT, (*specify a parenthetical expression*)

Filter Fields

The following table describes all of the possible Alert search fields. The fields listed in the first column correspond with results table column names. The field names listed in the second column are the fields you specify when you form field-based name-value pair search expressions.

> **Note:** Not all fields are included as columns in the results table. When you search by fields without column names, you can locate

the matching values in the details page. All of the fields listed in this table can be selected when you export results.

Column Name	Field Name	Type	Description
Age	age	Numeric	Indicates the age of the indicator in days. Event time - intel first seen A negative age value indicates that the event data was added to Anomali Security Analytics through backfill.
Alert Time	alert_time	Date	Timestamp when the alert was triggered. **Notes:** • In the results table, the time displayed is UTC time, adjusted for the browser time zone. • When you form search expressions, specify UTC time in the following format: <YYYY><MM><DD>T<HH>:<MM>:<SS>. The date part and the time part are separated by a capital T. You do not need to include T and the time values if you intend to search by date only. The following is an example of UTC time format: `2022-01-05T00:00:00` • You can also specify a time zone offset for searches where time zone precision is important. In the following example, the time zone offset is the `-08:00` at the end: `2022-01-05T00:00:00-08:00` • In exported results, the date and time are displayed as epoch time values. The following example shows the previous date-time example in epoch format: `1641342478`

Column Name	Field Name	Type	Description
Link Type	app_type	String	Link type that generated the event. Possible values: `universal_link`, `splunk`
ASN	asn	String	Autonomous System Number (ASN) for the IP associated with the indicator.
Criticality	asset_src_criticality	String	Criticality associated with the asset that is the source of a logged event. Possible values: `critical`, `high`, `medium`, `low`
Department	asset_src_dept	String	Assigned department for an asset that is the source of a logged event. Examples: `Engineering`, `Finance`, `HR`, `Labs`, `Marketing`
Hostname	asset_src_hostname	String	Host name for an asset that is the source of a logged event. Examples: `example.local`, `example-pc`
IP	asset_src_ip	String	IP address for an asset that is the source of a logged event. Example: `192.0.2.1`
Location	asset_src_location	String	Assigned location for an asset that is the source of a logged event. Example: `Redwood City, CA`
Vulnerability	asset_src_vulnerability	String	Vulnerability CVE number associated with an asset that is the source of a logged event. Examples: `CVE-2021-21137`, `CVE-2019-3385`
Classification	classification	String	Indicates the confidentiality level of an indicator. Possible values: `private`, `public` **Note:** Private also includes Trusted Circles.
Confidence	confidence	Numeric	Score from 0 to 100, as reported by the threat feed provider.

Column Name	Field Name	Type	Description
Count	count	Numeric	Aggregated number of events that matched the search criteria.
Country	country	String	Two-letter ISO country code for the IP associated with the indicator. For example, `US`, `CN`, `DE`, and so on.
DGA Probability	dga_prob	Numeric	*Relevant for email-specific events* Probability based on Anomali Security Analytics's DGA algorithm that the domain in the event is a DGA domain.
DGA TAG	dga_tag	String	Tags associated with the DGA domain that can be used to search for it.
	do_alert	Boolean	Link alerts. Whether the option to send alerts when Link becomes available has been selected.
Action	event.action	String	*Relevant for firewall and web proxy events* Event log action taken by the source device; for example, `Deny`, `Accept`.
Answer	event.answer	String	Answers for the DNS query. Example: `["10.10.10.10","10.10.10.11"]`
Application	event.app	String	The application detected. Example: `Slack`, `Google Gmail`, `LinkedIn`
Bytes In	event.bytes_in	Numeric	How many bytes received by a network interface. Example: `347`
Bytes Out	event.bytes_out	Numeric	How many bytes transmitted by a network interface. Example: `665`
Category	event.category	String	*Relevant for AWS VPC and Microsoft Defender logs.* Traffic direction: `ingress` or `egress`.

Column Name	Field Name	Type	Description
Command Line	event.command_line	String	The full command string of the spawned process. Example: `"\"procdump.exe\" -ma ls"`
Destination	event.dest	String	Event log destination data. The `event.dest` value populated from event logs is: • An IP address—for example, `192.0.2.1`. • A fully qualified domain name or registered domain name (second-level domain)—for example, `www.google.com` or `google.com`. • Host and domain data extracted from URL data. For example, if Security Analytics receives an event log with a destination URL `http://www.example.com/somepath/34839/jk30jf`, Security Analytics populates `event.dest` with the extracted host and domain `www.example.com`. Indicators that have IP or Domain value types can match `event.dest` values. See "ThreatStream Indicator Types" on page 1028 for a reference that includes indicator value types and descriptions. By default, Security Analytics correlates indicators and `event.dest` values.

Column Name	Field Name	Type	Description
Destination IP	event.dest_ip	String	Event log destination IP address. The `event.dest_ip` value populated from event logs is an IP address—for example, `192.0.2.1`. Indicators that have IP value types can match `event.dest_ip` values. See "ThreatStream Indicator Types" on page 1028 for a reference that includes indicator value types and descriptions. By default, Security Analytics correlates indicators and `event.dest_ip` values.
Destination Port	event.dest_port	Numeric	Event log destination port. Event log destination port field. The value for `event.dest_port` is the port number from the destination host—for example, `80`.
Data Source ID	event.ds_id	Numeric	For Universal Link log sources, this is the log source configuration ID. For Splunk log sources, this field is not applicable.
Data Source Type	event.ds_type	String	Event log data source type. Examples: `az_sentinel`, `qradar`
Event ID	event.event_id	String	A Windows identification number that specifies the event type. Example: `4624`
Event Name	event.event_name	String	The name of an event. Example: `DnsRequest`, `ProcessRollup2`

Column Name	Field Name	Type	Description
Filehash	event.file_hash	String	Event log file hash field. For example, an endpoint management application might write a log that contains file hash values. The `event.filehash` value populated from event logs is a hash value—for example, `69efa658c59d884c0cd6164cbb61d6d0cb0174355dc9c69327dfb76237c9c9c4`. Indicators that have Hash value types can match `event.filehash` values. See "ThreatStream Indicator Types" on page 1028 for a reference that includes indicator value types and descriptions. By default, Security Analytics correlates indicators and `event.filehash` values.
	event.file_hash2	String	A log might have multiple file hash fields.
	event.file_hash3	String	A log might have multiple file hash fields.
File Name	event.file_name	String	Event log field containing filepath.
File Path	event.file_path	String	The folder containing the file. Sigma name: FilePath Example: `C:\Program Files (x86)\VMware\VMware Workstation`
Originated Host	event.host	String	Event log hostname field. For example, for events ingested from Splunk Link, the value for `event.host` is the hostname of the Splunk indexer that forwarded the event.
HTTP Method	event.http_method	String	The HTTP method used in the request. Example: `get`, `post`, `delete`, `patch`

Column Name	Field Name	Type	Description
HTTP Referrer	event.http_referrer	String	The HTTP referrer used in the request. Example: `https://example.com/` Note: Correlated with indicators of type url.
Image	event.image	String	The executable name of the process. Sigma name: Image, ProcessName, OriginalFileName, TargetImage, TargetFileName Example: `svchost.exe`
Message ID	event.message_id	String	The globally-unique message identifier. Example: `123e4567-e89b-12d3-a456-426655440000`
Original File Name	event.original_file_name	String	Original name of the file that was changed. Example: `"test.pdf"`
Parent Command Line	event.parent_command_line	String	The full command string of the parent process. Example: `C:\Windows\System32\svchost.exe -k WerSvcGroup`
Parent Image	event.parent_image	String	The executable name of the parent process. Example: `notepad.exe`
Parent Process ID	event.parent_process_id	String	The numeric identifier of the process assigned by the operating system. Example: `4834`
Platform	event.platform	String	The operating system of the asset. Sigma name: Platform Example: `win`, `mac`, `linux`
Process ID	event.process_id	Numeric	The numeric identifier of the process assigned by the operating system. Example: `3683`

Column Name	Field Name	Type	Description
Protocol	event.protocol	String	*Relevant for firewall and web proxy events* Event log protocol field. The value for `event.protocol` is the network protocol used to make the connection to the source device—for example `http`.
DNS Query	event.query	String	The domain that needs to be resolved in a DNS query. Example: `www.google.com` Note: Correlated with indicators of type domain.
Email Receiver	event.receiver	String	*Relevant for email-specific events* Event log receiver field. The value for `event.receiver` is the receiver's email address, as specified in the To: field of the email—for example, `user@example.com`. Indicators that have Email value types can match `event.receiver` values. See "ThreatStream Indicator Types" on page 1028 for a reference that includes indicator value types and descriptions. By default, Security Analytics correlates indicators and `event.receiver` values.
Record Type	event.record_type	String	The DNS resource record type. Example: `A`, `CNAME`, `MX`, `NS`, `PTR`, `AAAA`
Registry Key	event.reg_key	string	Registry key that the recorded action was applied to. Sigma name: TargetObject Example: `HKEY_LOCAL_MACHINE\SOFTWARE\RegisteredApplications`
Registry Value Name	event.reg_value_name	string	Name of the registry value that the recorded action was applied to. Example: `"Wordpad"`

Column Name	Field Name	Type	Description
Registry Value Data	event.reg_value_data	string	Data of the registry value that the recorded action was applied to. Example: `Software\Microsoft\Windows\CurrentVersion\Applets\Wordpad`
Email Sender	event.sender	String	*Relevant for email-specific events* Event log sender field. The value for `event.sender` is the sender's email address, as specified in the From: field of the email—for example, `user@example.com`. Indicators that have Email value types can match `event.sender` values. See "ThreatStream Indicator Types" on page 1028 for a reference that includes indicator value types and descriptions. By default, Security Analytics correlates indicators and `event.sender` values.
Source Type	event.sourcetype	String	Source device type that generated the event.
Event Source	event.src	String	Event log source IP field. The `event.src` value populated from event logs is: • An IP address—for example, `192.0.2.1`. • A fully qualified domain name or registered domain name (second-level domain)—for example, `www.google.com` or `google.com`. Indicators that have IP type or Domain value types can match `event.src` values. See "ThreatStream Indicator Types" on page 1028 for a reference that includes indicator value types and descriptions. By default, Security Analytics correlates indicators and `event.src` values.

Column Name	Field Name	Type	Description
Source IP	event.src_ip	String	Event log source IP field. The `event.src_ip` value populated from event logs is an IP address—for example, `192.0.2.1`. Indicators that have IP value types can match `event.src_ip` values. See "ThreatStream Indicator Types" on page 1028 for a reference that includes indicator value types and descriptions. By default, Security Analytics correlates indicators and `event.src_ip` values.
Source Port	event.src_port	Numeric	*Relevant for firewall and web proxy events* Event log source port field. The value for `event.src_port` is the port number from the source device from which the connection was made—for example, `3022`.
	event.status	String	The status of the service.
Subject	event.subject	String	The subject of the message.
URL	event.url	String	*Relevant for firewall and web proxy events* Event log URL field. The value for `event.url` is populated from URL data having the form `http(s)://<FQDN (registered domain)>:[<port>]/[path]?[<query_params>]`—for example, `http://www.example.com:443/` or `http://www.example.com/somepath/34839/jk30jf`. Indicators that have URL value types can match `event.url` values. See "ThreatStream Indicator Types" on page 1028 for a reference that includes indicator value types and descriptions. By default, Security Analytics correlates indicators and `event.url` values.

Column Name	Field Name	Type	Description
User	event.user	String	*Relevant for firewall and web proxy events* Event log user field. The value for `event.user` is the username associated with an authenticated HTTP(S) connection request—for example, `user@example.com`.
User Agent	event.user_agent	String	Event log user agent field. The value for `event.user-agent` is user-agent directive data in an HTTP(S) connection request—for example, `Mozilla/5.0 (platform; rv:geckoversion) Gecko/geckotrail Firefox/firefoxversion`.

Column Name	Field Name	Type	Description
Event Time	event_time	Date	Event log timestamp field. The value for `event.time` is timestamp when the event was generated on the source device—for example, `2021-07-28T19:20:00`. **Notes:** • In the results table, the time displayed is UTC time, adjusted for the browser time zone. • When you form search expressions, specify UTC time in the following format: <YYYY><MM><DD>T<HH>:<MM>:<SS>. The date part and the time part are separated by a capital T. You do not need to include T and the time values if you intend to search by date only. The following is an example of UTC time format: `2022-01-05T00:00:00` • You can also specify a time zone offset for searches where time zone precision is important. In the following example, the time zone offset is the `-08:00` at the end: `2022-01-05T00:00:00-08:00` • In exported results, the date and time are displayed as epoch time values. The following example shows the previous date-time example in epoch format: `1641342478`
Indicator	indicator	String	Value of the indicator. This field contains the value that was matched and is always equal to the value of srcip, url, domain, md5, or email fields.
IOC Type	indicator_type	String	Data type of the indicator. Possible values: `ip`, `domain`, `url`, `email`, `md5`

Column Name	Field Name	Type	Description
iType	itype	String	Indicator type. For example, `c2_ip`, `compromised_email`, `apt_md5`, and so on. See "ThreatStream Indicator Types" on page 1028 for a complete list of available indicators.
	last_activetime	Date	Link alerts. Time events were received from a Link.
Latitude	lat	Numeric	Latitude associated with the Geo location of the IP. The value displayed is rounded up to the nearest thousandth decimal place. For example: 32.789. **Note:** Search results are based on non-rounded values, so you might observe anomalous search results, such as a search for `lat = 32.789` does not return a result showing a result value `32.789` but a search for `lat <= 37.789` does show a result for `32.789`. Be aware that rounding produces such minor anomalies.
	link_id	String	Link alerts. Link ID.
	link_name	String	Link alerts. Link configuration name.
	link_type	String	Link alerts. Link type.

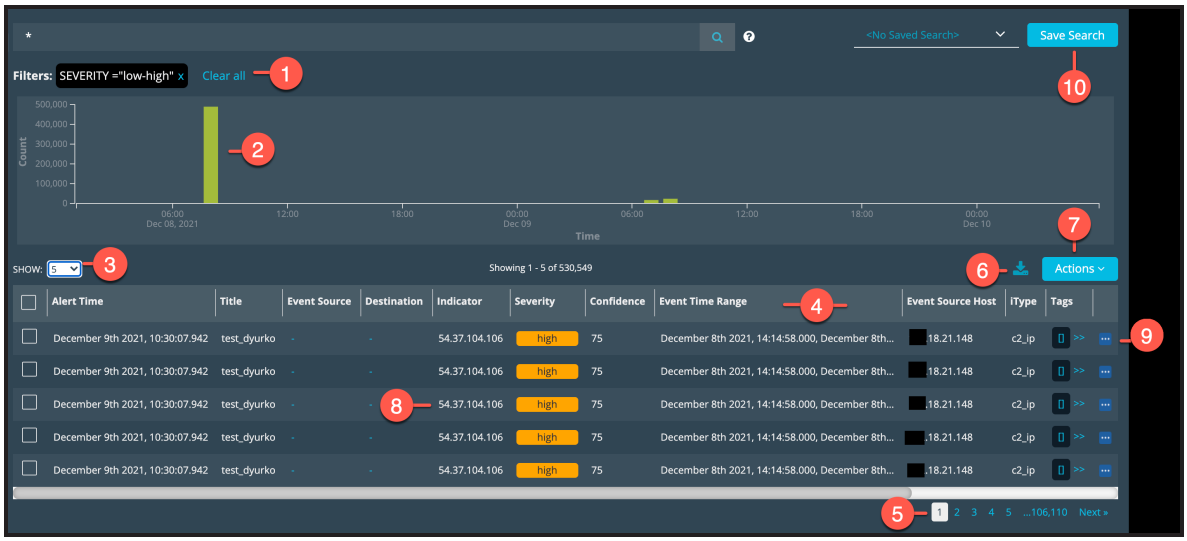
Column Name	Field Name	Type	Description
Longitude	lon	Numeric	Longitude associated with the Geo location of the IP. The value displayed is rounded up to the nearest thousandth decimal place. For example: 16.366. **Note:** Search results are based on non-rounded values, so you might observe anomalous search results, such as a search for `lon = 16.366` does not return a result showing a result value `16.366` but a search for `lon <= 16.366` does show a result for `16.366`. Be aware that rounding produces such minor anomalies.
Malware Family	malware_family	String	One or more public malware family names expected to have originated the domain. **Note:** Malware families are often known by multiple names or aliases. The name shown in the Anomali Security Analytics UI is one of those names or aliases.
	match_count	Numeric	Sum of events included in the alert.
	match_description	String	Link alerts. Alert message.
Event Time Range	match_records_time_window	Date	The time window examined by the alert rule. `2021-11-29T07:22:14+00:00`
Match Type	match_type	String	Type of alert query filter that matched. Example: `actor`
	originator	Numeric	Indicates whether the connection was inbound or outbound • 0 indicates inbound • 1 indicates outbound

Column Name	Field Name	Type	Description
Severity	severity	String	Severity associated with the threat feed that supplied the indicator. Possible values: `low`, `medium`, `high`, `very-high` **Note:** The search index is tokenized. This means the text is broken down into individual terms during indexing to allow for partial matching. For example, searches for `severity=high` returns matches for both `high` and `very-high`. If the tokenized search behavior returns unexpected results, you can form your search expression for this field using *`fieldname`*`.raw`. For example, if you want results for `high`, not including `very-high`, specify `severity.raw=high`. For more information, see "Getting Started with Activity Search" on page 57.
Source	source	String	Name of the feed provider or organization that reported the indicator.
Feed	source_feed_id	Numeric	Identifier associated with the feed that contained the indicator.
Event Source Host	src_host	String	An event source host value derived from asset_src_hostname, event.src, or event_ip fields, in that order. The hostname provided by the asset enrichment would be most readable, so if it data exists for it, it is used. If not, then the other source fields are evaluated.
State	state	String	Current state of the indicator as reported by the threat feed. Possible values: `active`, `inactive`, `falsepos`
Tags	tags	String	Tags specified in the alert rule configuration. For link alerts, the tags field is populated with the Link ID (dcid) and a message indicating one of the following statuses: `No events received` or `Link restored`.

Column Name	Field Name	Type	Description
TM ids	tm_ids	Numeric	Threat Model ID information from ThreatStream.
TM names	tm_names	String	Threat Model name information from ThreatStream.
TM type	tm_type	String	Threat Model type information from ThreatStream.
	trusted_circle_names	String	Names of the Trusted Circle with which this threat intelligence is shared on ThreatStream. **Note**: This field, not trusted_circle_id, is included in the export file when you export search results.
Raw Event ID	_raw_id	Numeric	Internal.

Alerts Match Results Table

The following figure identifies the UI elements that you use to manipulate the displayed results to find information about Alerts matches.



1	Review and reset applied filters.

2	Observe the graph of matches over time.
3	Select a number of rows per page.
4	Click the column header to sort the rows in ascending or descending order according to values in the column. Click a column header divider and drag it to make a column wider or more narrow.
5	Go to the next page of results or another page by page number.
6	Export the results table. See "Export Search Results" on page 66.
7	Perform an action related to the selected row. See "Perform Actions" below.
8	Click a hyperlinked indicator value and select an action: search VirusTotal or run a retrospective search.
9	Display the Details page for the matched event. See "View Alert Details" on the next page.
10	Create a Saved Search configuration. See "Saved Searches" on page 65.

Perform Actions

The Action menu above the results table allows you to perform the following actions.

Action	Description
Configure Fields	Select this option to configure the fields (columns) that appear in the results table.
Retrospective Search	Select this option to perform a retrospective search for the indicator correlated with the event. **Note**: This action is not applicable for Link alerts.

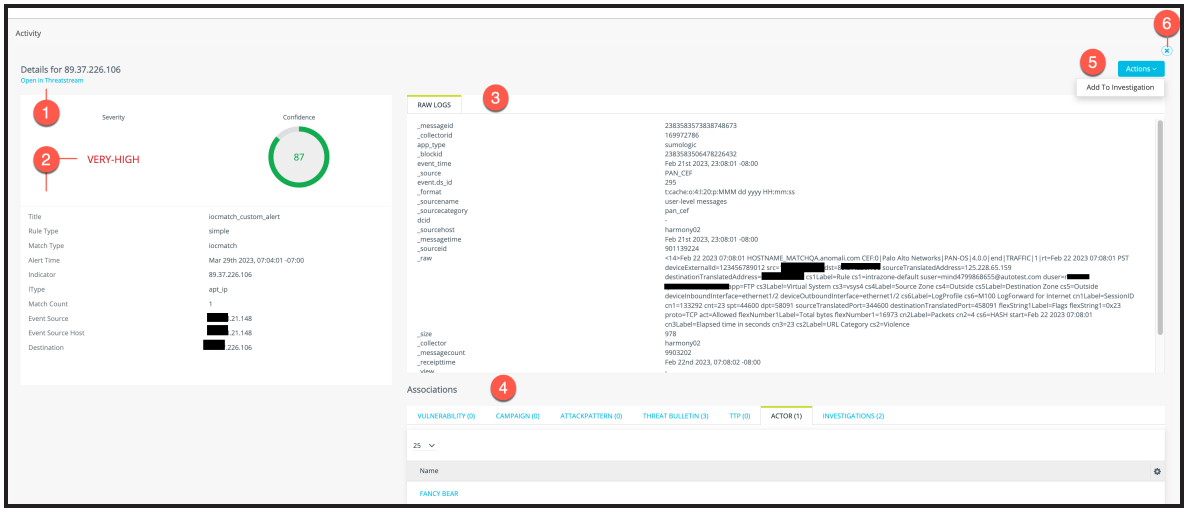
Action	Description
Investigate	Select this option to add the result to a ThreatStream investigation. Configure one of the following choices: • **Create Investigation**: Specify a name for the investigation and select an assignee to create a ThreatStream investigation. • **Add to Investigation**: Search or browse to find and then select a ThreatStream investigation. **Note:** For information about ThreatStream investigations, refer to the ThreatStream online help.

View Alert Details

	Click the Details icon in the right-most column to display the details page.

Alert Details for IOC Matches

The following figure identifies the UI elements that you use to find information on the Alert Details page.

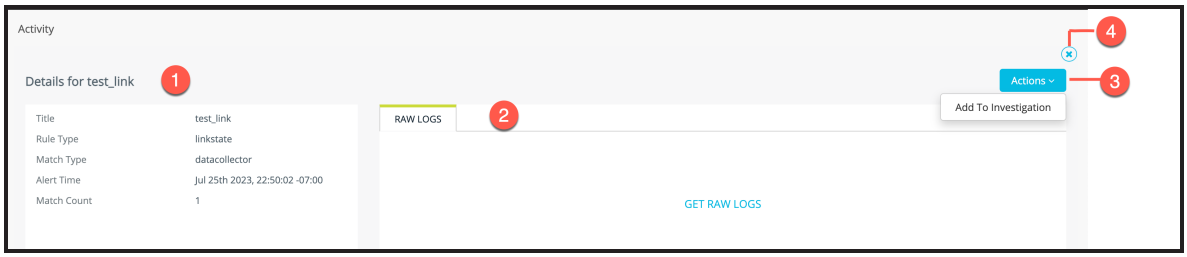


1	Open ThreatStream to view ThreatStream reports about the indicator.
2	Review the indicator details and event details correlated in Security Analytics.

3	**Raw Logs**: View more event data. When you click **Get Raw Logs**: • Security Analytics sends a drilldown query to log sources that support drill down queries. The source sends the raw log in response. Raw logs are available as long as they remain available on the log source system. • Security Analytics retrieves event log data from Security Analytics storage for log sources that do not support drilldown queries. The fields in logs stored in Security Analytics have been normalized to Security Analytics event fields. • Security Analytics returns no results if the associated Anomali Link is inactive.
4	Use the tabs to review associated ThreatStream threat model entities and investigations.
5	Click **Actions** and select **Add to Investigation** to add the log to a ThreatStream investigation. **Note:** For information about ThreatStream investigations, refer to the ThreatStream online help.
6	Click the **X** to exit the details page and return to the results table.

Alert Details for Link Alerts

The following figure identifies the UI elements that you use to find information on the Alert Details page.



1	Review the Link alert rule and matching event details.
2	Click **Get Raw Logs** to see the alert message JSON content.

3	Click **Actions** and select **Add to Investigation** to add the log to a ThreatStream investigation. **Note:** For information about ThreatStream investigations, refer to the ThreatStream online help.
4	Click the **X** to exit the details page and return to the results table.

Alert Details for Event Search Alerts

Alert details works differently for Event Search alerts. When you click the Details icon , Security Analytics opens a new browser tab to Event Search and loads the Event Search query and time range that was specified in the alert rule that was triggered. From there, you can modify the query as desired to hone in on details related to the condition that triggered the alert.

Asset Activity Searches

Search the Asset index to examine IT asset details imported into Security Analytics during the specified time period. The Asset details page shows a history of IOC matches associated with the asset.

1	**Search text box**: Specify a keyword or field-based search expression. Keyword searches match any field. Specify field-based name-value pairs for more precise targeting.
2	**Applied Filters**: Review and clear filters.

About Asset Searches

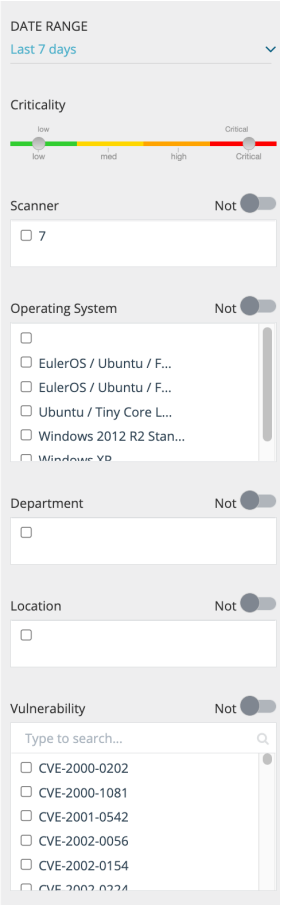
An *asset model* in a network infrastructure defines attributes of computer assets (a device, server, software). Attributes can include IP addresses, hostnames, MAC addresses, criticality, geographic location, and so on. For example, the servers in a finance server farm of your company are highly critical assets. Therefore, IP addresses and MAC addresses associated with those servers can be labeled highly critical. Additionally, if this server farm is located in a data center in Virginia, you can also associate Virginia Data Center as the geographic location for the server farm.

You can upload an asset model of your network infrastructure to Security Analytics, so event matches are enriched with this information.

After you have uploaded an asset model to enrich Security Analytics, you can use Activity search to quickly identify impacted systems and prioritize the resources you want to spend on corrective measures. For example, you can leverage the asset enrichment to identify hosts impacted by security events by hostname rather than IP address, which can be very dynamic in DHCP environments. You can also leverage asset criticality attributes to help you prioritize risk analysis.

Filter UI

You can use the filter UI to apply the following filters to your search:



- **Date Range**
  Select a time period, a relative expression, or a date range. The time period filter is based on the Security Analytics asset record time; in other words, the timestamp the asset record was created in Security Analytics from its scanner source, CSV import, or manual entry.
- **Criticality**
  Use the slider to specify a criticality range or drag both ends of the slider to a single severity to filter on just one. Criticality is set by the asset data source.
  - Low
  - Medium
  - High
  - Critical
- **Scanner**
  - AWS
  - qualys
  - rapid7_insightvm_platform
  - tenable.io
  - tenable.sc
- **Operating System**
  Select one or more operating systems.
- **Department**
  Select one or more department names.
- **Location**
  Select one or more locations.
- **Vulnerability**
  Select one or more vulnerability CVE IDs.

> **Note:** You can use negation in search expressions by selecting the **NOT** operator next to the filter heading. For example, to use negation with Vulnerabilities, select the CVE IDs you do not want

to search and toggle on the **NOT** operator next to the Vulnerabilities filter heading.

Filter Examples

```
platform=windows
vulnerabilities in [CVE-2021-21137, CVE-2019-3385]
criticality=high AND (hostname startswith q or hostname startswith u)
platform contains *n*x and ip insubnet 192.0.2.0/24
timestamp >= 2021-01-01T00:00:00 AND criticality = critical OR criticality = medium
hostname contains VM and criticality = critical and vulnerabilities contains 2019
criticality = critical AND platform != ipad AND platform != macos AND platform != printer
((platform != "printers" AND criticality = "critical") OR (platform = "printers" AND criticality = "high")) AND vulnerabilities contains "CVE-1999.*"
timestamp >= "2021-01-01T00:00:00"
ip=192.0.2.1
ip insubnet 192.0.2.0/24
ip insubnet 192.0.2.0/24 and platform contains macOS
```

Filter Operators

The following table describes the logical operators you can use to form complex field-based search expressions. Operator names are **not** case sensitive.

Field Type	Use this Operator
String	=, !=, contains, startswith, insubnet, in (for lists)
Numeric	=, !=, <, <=, >, >=, in (for lists)
Date	=, !=, <, <=, >, >=
Logical	AND, OR, NOT (*specify a parenthetical expression*)

Filter Fields

The following table describes all of the possible Asset search fields. The fields listed in the first column correspond with results table column names. The field names listed in the second column are the fields you specify when you form field-based name-value pair search expressions.

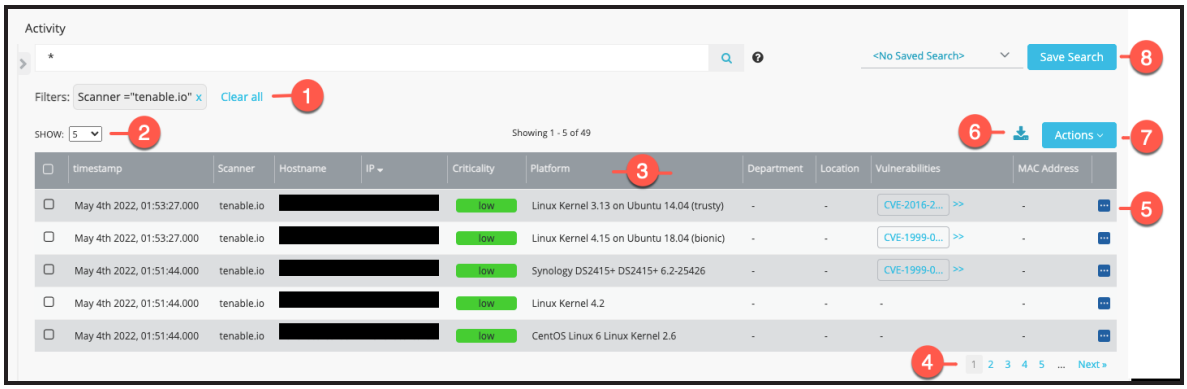
Column Name	Field Name	Type	Description
Criticality	criticality	String	Criticality associated with the asset. Possible values: critical, high, medium, low
Department	department	String	Assigned department. Examples: Engineering, Finance, HR, Labs, Marketing
Hostname	hostname	String	Host name. Examples: example.local, example-pc
IP	ip	String	IP address. Example: 192.0.2.1
FQDNS	fqdns	String	Fully-qualified domain name. Tenable.io scanner reports include a FQDN field for assets. Example: example.com
Location	location	String	Assigned location. Example: Redwood City, CA
MAC Address	mac	String	MAC address. Examples: 00:00:5E:EF:10-00:00:00
Netbios	netbios	String	NetBIOS is a program used to enable applications on separate computers to communicate within a LAN. Tenable.io scanner reports include NetBios data. Example: COMPUTERNAME1
Owner	owner	String	Owner field, if any, mapped from an AWS asset source.

Column Name	Field Name	Type	Description
Platform	platform	String	OS type. Examples: CentOS Linux, ipad, Linux-Ubuntu-18, macOS Mojave, printer, Windows XP, Windows NT 10.0
Scanner	scanner	String	A supported scanner from which the asset information was imported. Examples: qualys, rapid7_insightvm_platform, tenable.io, tenable.sc
	source	Numeric	ID of the scanner from which the asset data was imported. For example, if you had two Qualys scanners, the sources of information could be distinguished with source id=1 and source id=2.
Tags	tags	String	Tags field, if any, mapped from an AWS asset source.

Column Name	Field Name	Type	Description
timestamp	timestamp	Date	**Notes:** • In the results table, the time displayed is UTC time, adjusted for the browser time zone. • When you form search expressions, specify UTC time in the following format: <YYYY><MM><DD>T<HH>:<MM>:<SS>. The date part and the time part are separated by a capital T. You do not need to include T and the time values if you intend to search by date only. The following is an example of UTC time format: `2022-01-05T00:00:00` • You can also specify a time zone offset for searches where time zone precision is important. In the following example, the time zone offset is the `-08:00` at the end: `2022-01-05T00:00:00-08:00` • In exported results, the date and time are displayed as epoch time values. The following example shows the previous date-time example in epoch format: `1641342478`
Vulnerabilities	vulnerabilities	String	Vulnerability CVE number from asset datastore. Examples: CVE-2021-21137, CVE-2019-3385

Asset Match Results Table

The following figure identifies the UI elements that you use to manipulate the displayed results to find information about Asset matches.



1	Review and reset applied filters.
2	Select a number of rows per page.
3	Click the column header to sort the rows in ascending or descending order according to values in the column. Click a column header divider and drag it to make a column wider or more narrow.
4	Go to the next page of results or another page by page number.
5	Display the Details page for the matched event. See "View Asset Details" on the next page.
6	Export the results table. See "Export Search Results" on page 66.
7	Perform an action related to the selected row. See "Perform Actions" below.
8	Create a Saved Search configuration. See "Saved Searches" on page 65.

Perform Actions

The Action menu above the results table allows you to perform the following actions.

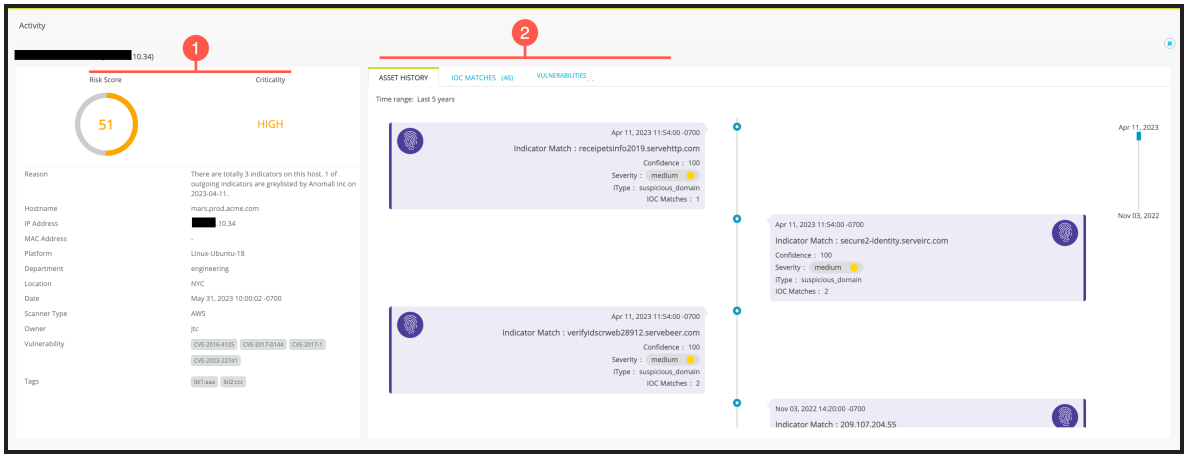
Action	Description
Configure Fields	Select this option to configure the fields (columns) that appear in the results table.
Retrospective Search	Select this option to perform a retrospective search for the indicator correlated with the event.

Action	Description
Add selected asset to exclude list	Select this option to add the asset to the asset exclude list.

View Asset Details

	Click the Details icon in the right-most column to display the details page.

The following figure summarizes the Asset Details page sections.



1	Review detailed items described in "Asset Details Listing" below.
2	Use the tabs to learn more: • **Asset History**: View a timeline of IOC matches. See "Asset History" on the next page. • **IOC Matches**: View an IOC match table. See "IOC Matches" on page 212. • **Vulnerabilities**: View a listing of matched vulnerabilities. See "Vulnerabilities" on page 213.

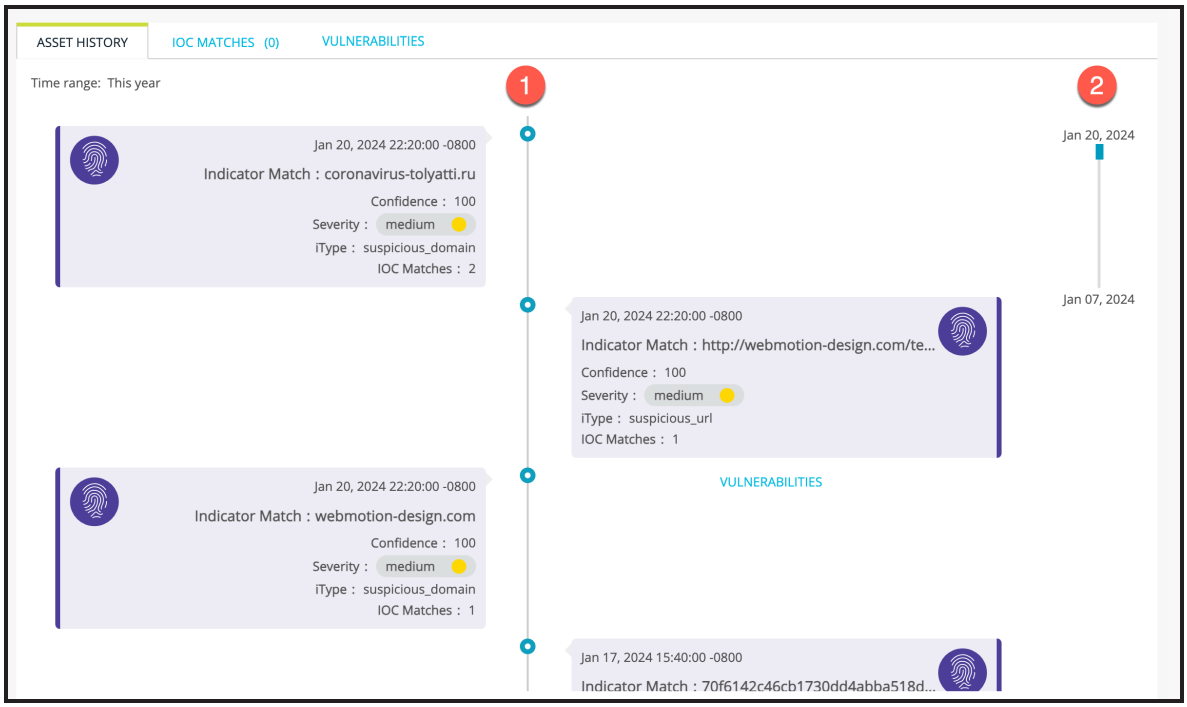
Asset Details Listing

The following table describes the asset details items.

Item	Description
Risk Score	Risk score is a weighted score based on multiple factors, including indicator confidence, severity, indicator type, and the number of sources reporting the indicator.
Criticality	Criticality set by the asset data source: • Low • Medium • High • Critical
Reason	An explanation about Risk Score when such detail is available.
Hostname	Hostname from the asset datastore.
IP Address	IP address from the asset datastore.
Platform	Platform from the asset datastore.
Department	Department from the asset datastore.
Location	Location from the asset datastore.
Date	The timestamp the asset record was created in Security Analytics from its scanner source, CSV import, or manual entry.
Scanner Type	Scanner type from the asset datastore.
Owner	Owner field, if any, mapped from an AWS asset source.
Vulnerability	Vulnerabilities from the asset datastore.
Tags	Tags, if any, mapped from an AWS asset source.

Asset History

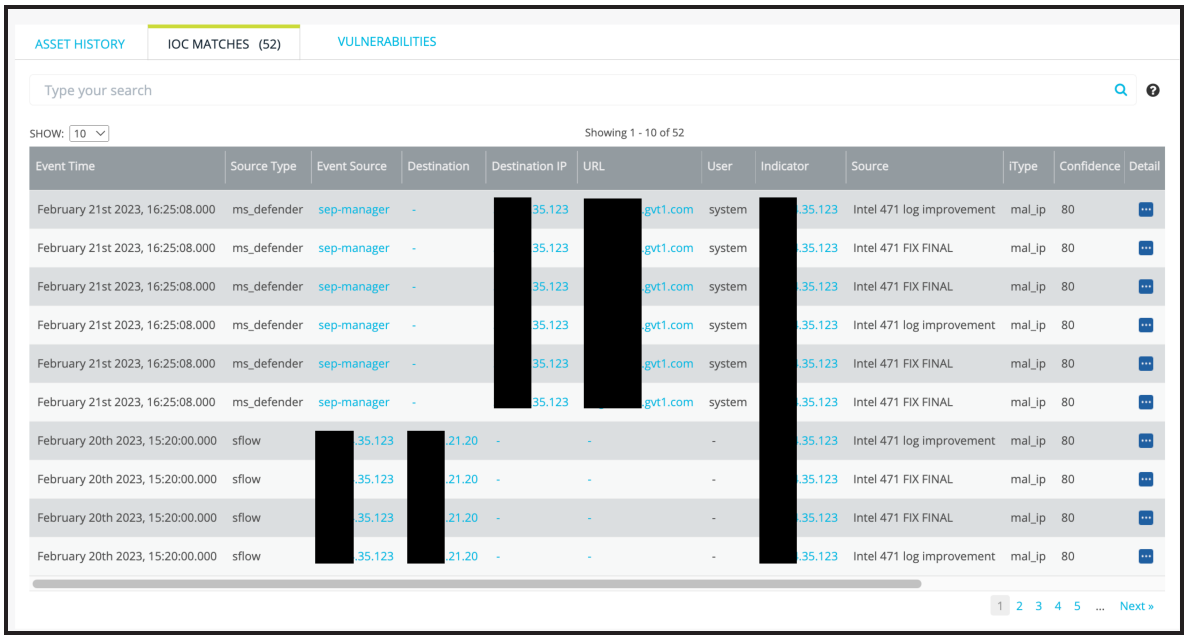
The following figure shows the **Asset History** tab.



1	**Timeline**: Review events that matched IOCs in the timeline. Click an event to issue a search on the IOC Match activity search, filtered for the particular asset host and matching IOC rule.
2	**Scroll Bar**: Use the scroll bar to scroll the timeline if necessary.

IOC Matches

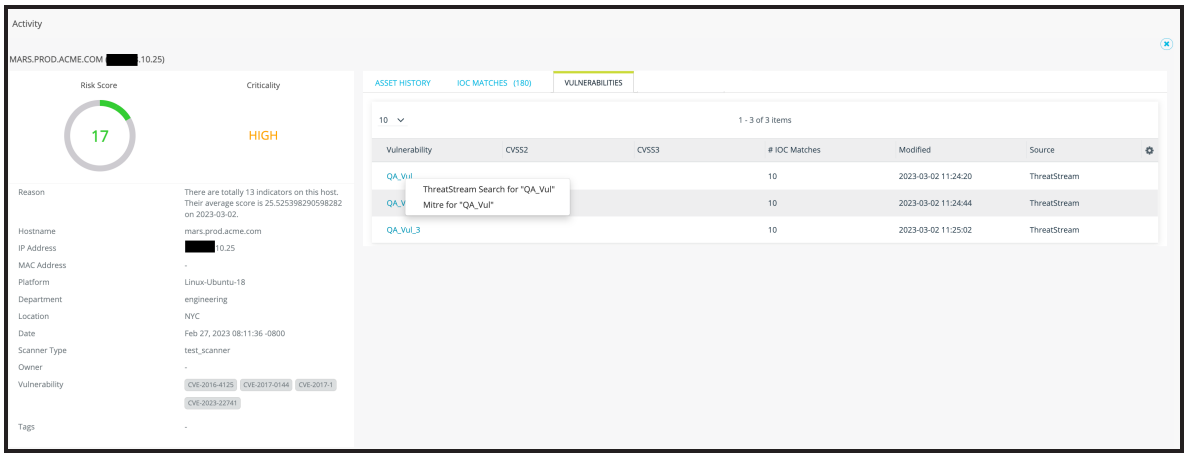
The following figure shows the **IOC Matches** tab.



The IOC Matches results table can be used just like the IOC Match activity search results table. For details, see "IOC Match Results Table" on page 90.

Vulnerabilities

The following figure shows the **Vulnerabilities** tab. The **Vulnerabilities** tab data is populated by ThreatStream intelligence, not the asset datastore. This tab shows a summary of CVSS scores and the source of this information.



You can click the hyperlink in the Vulnerability column and select **ThreatStream Search** or **Mitre** to go to additional details hosted on ThreatStream or cve.mitre.org.

Chapter 4: Managing Saved and Scheduled Configurations

Analysts routinely configure alerts and saved searches, schedule retrospective searches, generate and schedule reports, export search results, add false positives or other exceptions to exclude lists, and update Event Search lookup tables.

Both analysts and administrators can use the **Manage** menu to perform the following activities:

- Review, delete, or modify configurations
- Download generated reports
- Download search result export files
- Manage lookup tables

Using Alerts

Anomali alerts automate the detection and response process for security events that meet user-defined conditions. By continuously monitoring large volumes of event data, alerts ensure that relevant security signals trigger notifications and response workflows with minimal manual intervention.

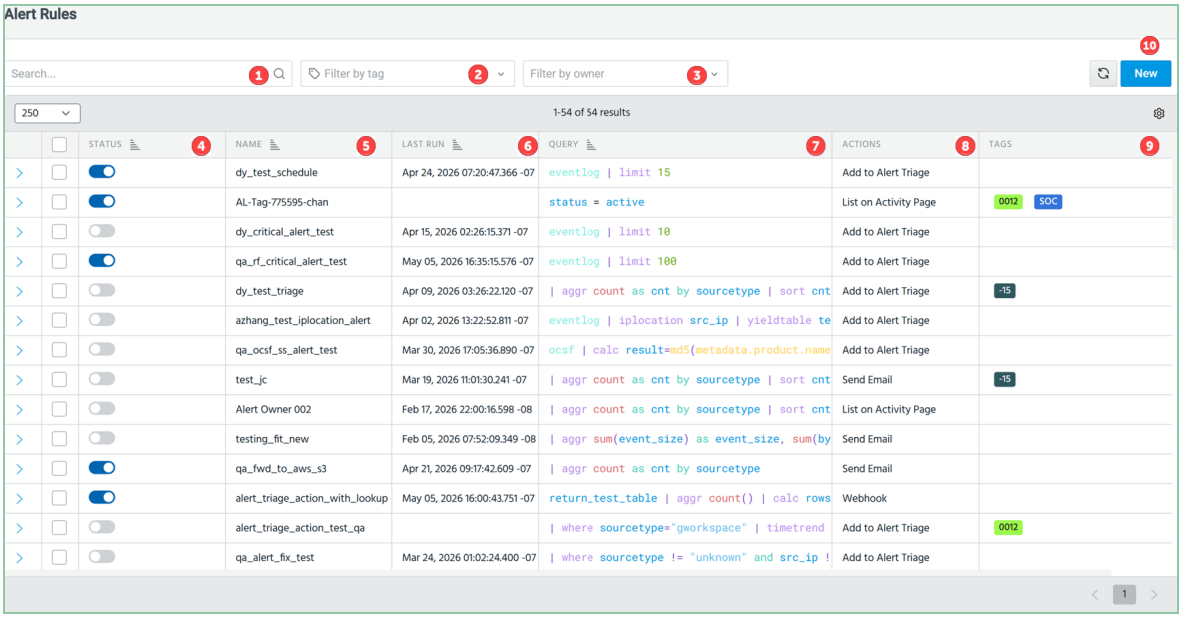
Alert rules define the conditions, schedules, and actions associated with each alert. When triggered, alerts can automatically execute configured actions such as sending email notifications, forwarding events to external systems, or adding matched data to ThreatStream investigations, among several others. An organization can configure a maximum of up to 250 alert rules.

These automated workflows help analysts stay informed about critical events without needing to remain logged in to the platform, enabling efficient monitoring and investigation.

Alerts support both the eventlog and OCSF Version 1.2 schema fields with dotted notation. See OCSF Schema Overview for more information on the OCSF fields and naming conventions.

Overview

To set up an alert, on the Anomali menu, navigate to **Alerting** > **Manage** > **Alert Rules**.



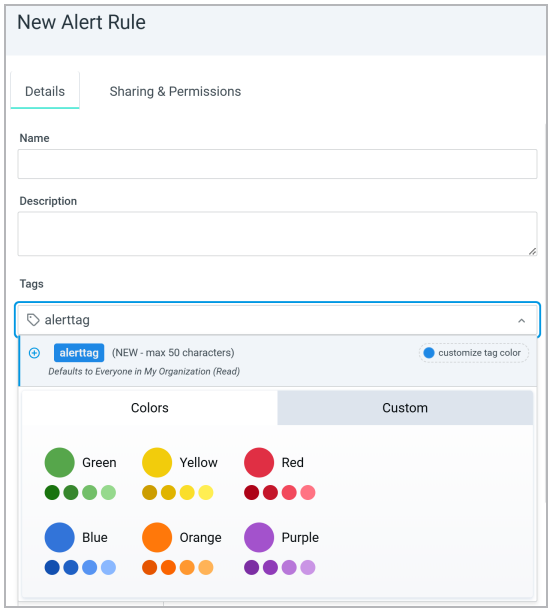
1	**Search bar**: Search for an alert by its name. The search incrementally filters the table as you type the name or values from other columns.
2	**Filter by tag**: Filter the alert list by one or more resource tags. • The tag filter drop-down shows only tags you own or that are shared to your organization. Organization administrators can also see private tags owned by other users. • When you select multiple tags, only alerts that have all selected tags applied are returned. • The count next to each tag shows how many alerts have that tag applied, not the total across all the supported resource types. See "Filtering Alerts by Resource Tag" on page 251 for details.

3	**Filter by owner**: Filter the alert table based on the owner of an alert. **Note:** A user can view, edit, or clone alerts they create. See "User Sharing and Permissions" on page 219 for more information.
4	**Status**: Toggle the status switch to enable or disable an alert.
5	**Name:** Displays the name of the alert. Each alert must have a unique name.
6	**Last Run:** Shows the most recent date and time the alert was triggered.
7	**Query:** Captures the AQL query used to configure an alert. You can enter an AQL query or you can use a saved search. Alerts support forensic searches.
8	**Actions:** Shows all the actions a triggered alert is configured to take.

9

Tags: Resource tags applied to an alert for filtering and organization.

- Click ⊕ to add tags to an alert.
- The auto-complete suggestion shows tags you own and tags shared to your organization. Private tags associated with other users are not shown, except to organization administrators.
- To create a new tag, type a name and click **Customize tag color** to set a color.



- A new tag is added to the shared tag list immediately, even if you abandon updating the alert.

- Only tag owners and users with write permission can add or remove tags. See Resource Tagging Permissions for more information.

10	**Start Time:** Denotes the start of the time range of the query used to configure the alert.
11	**End Time:** Denotes the end of the time range of the query used to configure the alert.
12	**Schedule**: Indicates the configured schedule of the alert.
13	**Timezone:** Denotes the timezone of the user configuring the alert.
14	**Trigger Condition:** Captures the condition that will trigger an alert.
15	**New:** Create a new alert.
16	**Refresh:** Click to force alert table refresh.

User Sharing and Permissions

All users can always view and edit alerts they own. They can see only alerts they are entitled to view, based on the permissions granted under the **Sharing & Permissions** tab.

If the **Sharing & Permissions** settings are configured as:

- **Private**—Only the owner of the alert can view and edit the alert. By default, if no sharing is specified, the alert is private.
- **Shared**—Users with specified roles can view and edit the alert, according to their assigned permissions.

Users with roles granted read permissions:

- Can view, clone, and export alerts they own. Can only view, but cannot edit, the alerts they do not own.

Users with roles granted write permissions:

- Can modify the alert, but not sharing or permission rights.

Users who own the alert:

- Can perform all actions, including editing ownership and permissions of the alerts they own.
- If no sharing is specified, by default, the alert is private (not shared).

Audit logging:

- All create, update, and delete actions are logged with details such as the timestamp or the alert action.
- Only org admins can access all audit trails to ensure reliable compliance.

Organization Administrators

- Can perform all actions, including editing ownership and permissions of any alert.
- Can access all audit trails.

Creating Alerts

Alerts run scheduled AQL queries that evaluate trigger conditions and automatically perform configured actions when the conditions are met. See "Creating Alerts" below for more information.

Set Alert Actions

Configure an alert to perform one or more actions when it triggers. See "Setting Alert Actions" on page 241 for more information.

Triage your Alerts

You can triage your alerts and investigate, prioritize, and manage triggered alerts. See "Alert Triage" on page 244 for more information.

Managing Alerts

You can edit, clone, or delete alerts. See "Managing Alerts" on page 250 for more information.

Creating Alerts

Alerts run scheduled event searches and trigger actions when results match defined conditions. Configured actions can send results to destinations such as email recipients, syslog receivers, or third-party systems through HTTP POST.

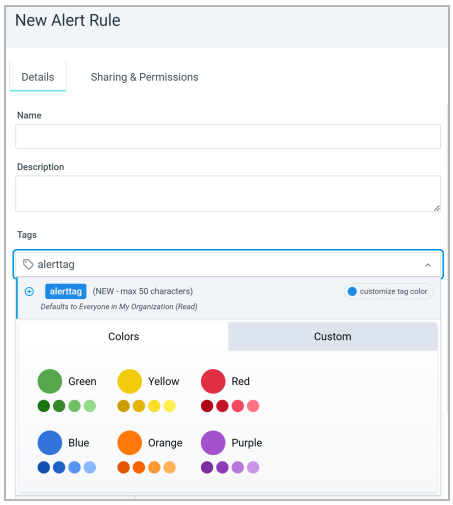
Alerts support both the eventlog and OCSF Version 1.2 schema fields with dotted notation. See OCSF Schema Overview for more information on the OCSF fields and naming conventions.

> **Note:** Any alert action will return the top 25,000 aggregated search results and 50,000 non-aggregated search results.

To create an alert:

1. Navigate to **Manage** > **Alerts** > **Alert Rules**.
2. Click **New**.
3. Configure the Source settings described in the following table.

Setting	Description
Name	Enter a name, using only ASCII characters.
Description	(Optional) Enter a description for the alert.
Mark as Critical Alert* (*Limited Availability option.)	This settings allows you to flag high-priority alerts that require guaranteed, timely execution. When enabled, the alert is routed to a dedicated, high-priority execution path designed to run as close to the scheduled time as possible. Since this path has finite capacity, marking too many alerts critical will increase contention in this path as well. Therefore, Anomali recommends using the **Mark as Critical Alert** setting for less than 10–15% of active alerts.

Setting	Description
Tags	(Optional) Enter or select resource tags to apply to the alert. a. Enter or select resource tags to apply to the alert. The auto-complete suggestion shows tags you own and tags shared to your organization. Private tags associated with other users are not shown, except to organization administrators. b. To create a new tag inline, type a name containing up to 50 characters and click **Customize tag color** to select a color. See Creating Resource Tags for details. A new tag is added to the shared tag list immediately, even if you abandon creating the alert. c. To apply an existing tag, type in the field and select it from the auto-complete suggestion results. d. Click **Manage Resource Tags** to view existing or newly created tags. 

Setting	Description
	Newly created tags default to **Everyone in my Organization (Read)**. Only tag owners and users with write permission can add or remove tags. See Resource Tagging Permissions for more information.

4. Complete the settings described in the following table.

Setting	Description
AQL Query	Provide an AQL query. Alerts support both the eventlog and OCSF Version 1.2 query fields with dotted notation. See OCSF Schema Overview for more information on the OCSF fields and naming conventions. ■ **Saved Search**: Select a saved search. If you use a saved search, changes you later make to that search also affect the alert. ■ **Custom**: Enter a valid AQL query or click the **History** icon ( ) to select a query from the **Search History** list.
Time Range	(Optional) Specify a time range for the search query. Possible ranges include the last one minute to the last 90 days, and more. By default, time range is **Last 1 hour**. You can also select quick search ranges that represent relative time ranges defined by default.

Setting	Description

Scheduling	(Optional) Determines how often the rule query runs. When the query results meet the alert condition, the system triggers the configured alert actions. You can configure the rule to run at predefined intervals or using a custom cron expression.
	
	Standard
	
	Run the rule at predefined intervals:
	
	▪ **Every minute**
	▪ **Every hour**
	▪ **Every 4 hours**
	▪ **Every 6 hours**
	▪ **Every day**
	▪ **Every week**
	
	Custom schedule
	
	Run the rule after a specified number of minutes, hours, or days.
	
	Cron schedule
	
	Run the rule using default or customizable cron expressions:
	
	▪ **Default**: Configure a cron job that runs every:
	  ◦ minute
	  ◦ hour–runs after the specified number of minutes past the hour
	  ◦ day–runs every day at the specified time (in

Setting	Description
	24-hour format) ◦ week–runs only on the specified day of the week at the specified time (in 24-hour format) ◦ month–runs on the specified day of the month (between 1-31) at the specified time (in 24-hour format) ▪ **Cron**: Schedule the cron job using a valid cron expression. For example, the cron expression `8 18 14 * *` runs the job at 6:08 PM on day 14 of every month. By default, an alert is assigned the **Standard: Every Hour** schedule.

Setting	Description
Alert if number of results	(Optional) Specify a condition that triggers the alert: ▪ **Is greater than**: Number of results exceeds the value specified in the rule. ▪ **Is less than**: Number of results is lower than the value specified in the rule. ▪ **Is equal to**: Number of results equals the value specified in the rule. ▪ **Is not equal to**: Number of results differs from the value specified in the rule. ▪ **Is greater than or equal to**: Number of results is greater than or equal to the value specified in the rule. ▪ **Is less than or equal to**: Number of results is less than or equal to the value specified in the rule. ▪ **Increases by**: Number of results increases by at least the specified value compared to the preceding interval. ▪ **Decreases by**: Number of results decreases by at least the specified value compared to the preceding interval. ▪ **Custom Query**: Enter an alert trigger condition as a custom query to append to the main query at the top (Saved Search or Custom). For example, if: ◦ Main Query: `eventlog | limit 10` ◦ Custom Query: `where severity="low"` (or `| where severity="low"`)

Setting	Description
	then the final query becomes: `eventlog | limit 10 | where severity="low"` By default, an alert is triggered if the number of results is greater than zero.
Throttle	(Optional) Prevent repeated alert triggers within a specified time window. If you enable throttling, configure the following settings: ▪ **Throttle Results Containing**: Select one or more fields whose values must match for throttling to occur. ▪ **Throttle for**: Specify the time window during which matching alerts are throttled. For example, selecting `dest_ip` and one day as the throttle window throttles alerts triggered for the same destination IP within that day. By default, throttling is disabled.

5. Click **Add** to configure one or more of the following actions:

Action	Setting	Description
List on Activity Page	**List on Activity Page**	Adds the alert to the search index used by **Activity** > **Alerts** page. When the alert is triggered, a new entry is added to the Alerts activity search index. From the **Activity** page, you can find alerts by filtering on the rule name. Click **Details** for the alert to issue a search with the alert rule search criteria. By default, listing on the **Activity** page is disabled.

Action	Setting	Description
Send Email	**To**	Type or select one or more email addresses.
	Subject	(Optional) Specify an email subject line. The default subject uses the `$alert.name$` variable to set the subject.
	Priority	(Optional) Assign a priority level to the alert. Possible values include **Lowest**, **Low**, **Medium**, **High**, and **Highest**.
	Message	(Optional) Specify a message body. The default message uses the `$alert.name$` variable as the message. The message body shows the alert rule name, the search string, search time range, the time the alert was triggered, and the trigger condition details. The alert message includes up to 1,000 rows.

Action	Setting	Description
	Include	(Optional) Specify what the alert email should include in the email body. Select one or more of the following: ■ **Alert events as an attachment** ■ **Alert rule name** ■ **Alert time** ■ **Search string** ■ **Event time range** ■ **Link to search results** ■ **Trigger conditions** ■ **Trigger value** ■ **Details of latest events**
	Attachment Types	(Optional) Attach a PDF or CSV file to the alert email, that will contain the details of the events that triggered the alert.

Action	Setting	Description
Forward to Syslog	**Format**	Format in which the alert will be sent. For Syslog or Splunk, select JSON. For ArcSight ESM or QRadar, select CEF. The alert message includes up to 1,000 rows. Default format: JSON
	Address	Host name or external IP address for the remote syslog server to which the alerts will be sent. Ask your syslog administrator for the external IP address. The syslog server must be configured to allow syslog communication from Security Analytics over the internet. Only supports syslog over TCP.
	Port	Listening port for the specified host. Ask your syslog administrator for the correct port. Default: `514`
	CA certs	Only supports secure syslog. Click **Browse** and upload the destination server CA certificate (ca.pem file) provided by your syslog administrator. The maximum size for the certificate file is 24 KB.
	Output Raw Only	If checked, forwards only the raw event output of the alert without its metadata fields. Use this option when the server truncates alerts that exceed the acceptable length.

Action	Setting	Description
Forward to Splunk HTTP Event Collector (HEC)	**Format**	Format in which the alert will be sent: JSON or CEF. The alert message includes a maximum of 1,000 rows. Default format: JSON
	Host	If your Splunk instance is Splunk Enterprise, specify the fully qualified domain name or IP address for the Splunk host. If your Splunk instance is Splunk Cloud, specify `http-inputs-<host>.splunkcloud.com`, where `<host>` is the Splunk Cloud Platform instance that runs HEC. For example, `http-inputs-anomali.splunkcloud.com`. Refer to Splunk documentation for more information.

Action	Setting	Description
	Port	Specify the port configured in the HTTP Port Number field in the Global Settings of the Splunk HEC. By default, both Splunk HEC and Anomali alerts use port `8088`. **Note:** The port for Splunk HEC is typically different from the port for the Splunk dashboard. For example, a Splunk instance can be set up to have the Splunk dashboard accessible at `192.168.10.124:8000` and the Splunk HEC port configured to accept data on port `8088`.
	Token	Copy the token value expected by the Splunk HEC. Refer to "Forwarding Alerts from Anomali Security Analytics to Splunk" in the *Anomali Link (for Splunk) Installation Guide* for an illustrated example.
	Output Raw Only	If checked, forwards only the raw event output of the alert, without its metadata fields. Use this option when the server truncates alerts that exceed the acceptable length. Selected by default.
	HTTPS Enabled	Select this option if HTTPS is enabled on the Splunk HEC. Selected by default.

Action	Setting	Description
Webhook	**URL**	Specify the URL of a third party to which the matched events will be sent through an HTTP POST request. The third party will receive the matched events as a JSON payload.
	Authorization Header	(Optional) Provide an authorization header.
	Custom Header	(Optional) Provide any custom header.
	Payload	Enter the payload the webhook will share in JSON format.
	Trigger for every match	Select **Trigger for every match** to make a single call for every alert trigger and for the third-party service to send one webhook call for each match in the results set. Selected by default.

Action	Setting	Description
Forward to Azure	**Directory (Tenant) ID**	Copy the Directory (Tenant) ID value in the Microsoft Entra application settings.
	Application (Client) ID	Copy the Application (Client) ID value in the Microsoft Entra application settings.
	Client Secret	Copy the generated secret for the Microsoft Entra application
	Data Collection Endpoint	Copy the log ingestion URL value in the data collection endpoint settings.
	Data Collection Rule	Copy the Immutable Id value in Data collection rule settings.
	Data Collection Rule Stream Name	Copy the stream name in the Data Collection Rule settings (JSON View). It represents the table in which the forwarded alerts will be stored. The stream name string includes the table name.
	Output Raw Only	If checked, forwards only the raw event output of the alert, without its metadata fields. Use this option when the server truncates alerts that exceed the acceptable length. Unchecked by default.

Action	Setting	Description
Add to Alert Triage	**Add Result Entry**	Select how the output of the triggered alert is captured. Possible values are: **1 Entry when the Alert is Triggered** (selected by default) ■ This option causes the triggered alert to return only one result (one row) as the output. ■ Useful when you need bulk triage, as in the following example scenarios: ◦ Aggregated summary alerts that aggregate 50 brute-force sign-in attempts. ◦ Monitoring the performance of an alert rule rather than individual threats. ◦ All output logs are related to a single event, such as, one threat actor scanning multiple hosts. **1 Entry for Every Result** ■ This option causes the alert to return as output one result (or one row) each time the alert is triggered. ■ This is the default behavior of the triggered alert. ■ Useful when you need per-trigger triage, as in the following example scenarios: ◦ *Single search with multiple independent threat indicators*: Search query matches 100 different

Action	Setting	Description
		suspicious IP addresses accessed in the logs. In this case, each IP might belong to a different threat actor or campaign, with a different result for each IP address. ◦ *Credential abuse or account anomalies*: A search for failed logins from unusual countries by different users. In this case, each username represents a different identity, and an analyst must determine if the login was a brute-force attempt, misconfiguration, or legitimate user. ◦ *Data Exfiltration*: Search query returns rows of users uploading large files to external domains. In this case, the analyst needs to validate if each transfer was business-approved or malicious. ■ Select Maximum Row Count: The maximum number of rows created every time the alert is triggered. By default, a triggered alert creates 10 rows. You can select a maximum of 1000 rows for a triggered alert.

Action	Setting	Description
	Status	Status that the creator of the alert wants to assign to the triggered alert. ■ **New**: A new rule is configured. ■ **Open**: A configured rule is still valid and is not completed. ■ **In Progress**: A configured rule is currently running. ■ **Custom**: Enter a custom status for the triggered alert, enclosing the value in `<<value>>`. ◦ For example: `<<running_alert>>`
	Risk Score	(Optional) An integer (1–100) that represents the risk associated with the triggered alert.

Action	Setting	Description
	Severity	(Optional) Indicates the severity of the triggered alert. ■ **Critical**: Indicates critical severity. ■ **High**: Indicates high severity. ■ **Medium**: Indicates medium severity. ■ **Low**: Indicates low severity ■ **Informational**: Indicates the informational nature of the severity. ■ **Custom**: Enter a custom value (number or string) as the severity for the triggered alert, enclosed in `<<value>>`. ◦ For example: `<<running_severity>>`
	Owner	(Optional) The email address of the owner of the triggered alert, which can be either the email of the creator or the analyst that will address this alert. **Note:** You need the appropriate permissions to add alert rules. See SSO and Role Management for more information.

Action	Setting	Description
	Assignee	(Optional) The email address to which the alert action is assigned, typically a security analyst. Org admins control this assignment on the Alert Triage Dashboard, to ensure only current employees are assigned an alert action.
	Add MITRE Association	(Optional) Add an association to the MITRE framework to send enhanced information about the event that triggers the alert and its impact. **Domain**: Select one of the MITRE ATT&CK domains from Enterprise, ICS, and Mobile, depending on the MITRE version. **Tactics**: Specify the type of tactics involved. For example, collection, command and control, or credential access. **Techniques**: Specify the type of technique involved. For example, the `T1003` technique refers to credential dumping that is used to extract login credentials from compromised systems.
	Add Entities	(Optional) Add information about event, asset, and identity entities as a JSON string. Here, the values are populated using the first row of the search results. For example, `event entity` can be `{"name": "<<hostname>>", "ip": "<<src_ip>>", "source": "<<source>>"}`.`

Action	Setting	Description
Forward to AWS S3	**S3 Bucket**	URI of the S3 bucket to which the alert will forward the alert payload. For example: `s3://test_bucket/folderA/...`
	Access Key	Enter the Access key of the S3 bucket.
	Secret Key	Enter the S3 Secret Access Key.
	Output Format	Select an output format for the alert payload, either JSON or CEF.
	Output Raw Only	(Optional) If selected, forwards only the raw event output of the alert, without its metadata fields.

6. Click **Create** to finish creating the alert.

Setting Alert Actions

This page explains all the actions you can configure for each alert rule.

List on Activity Page

Adds the alert to the search index used for the **Activity** > **Alerts** page.

Send Email

Triggered alerts send email notifications, based on the configured alert schedule. The system sends the email through the AWS Simple Email Service (SES).

Forward Syslog

Forwards the matched events to a specified Syslog destination.

> **Note:** Security Analytics supports only secure syslog. When you configure the connection to the destination syslog server, specify the remote server external IP address and listening port. You must also upload the destination server CA certificate (cert.pem). The maximum certificate file size is 24 KB.
>
> Contact your syslog administrator to obtain the external IP address, listening port, and cert.pem file required to complete the configuration.

Forward to Splunk HTTP Event Collector

Forwards matched events to a specified Splunk HTTP Event Collector (HEC) destination. Anomali recommends forwarding alerts to Splunk HEC instead of Splunk syslog TCP input.

Webhook

Forwards matched events to a third-party service as a customizable JSON payload through an HTTP POST request. For example, you can use a webhook connection to create a ServiceNow ticket after Security Analytics triggers an alert. To set up a webhook connection:

- Navigate to **Manage** > **Alerting** > **Alert Rules**.
- Click **Add**.
- Configure the following alert specifications:
  - Name and description
  - Search type — Saved Search or Custom search
  - Event time range
  - Alert schedule
  - Alert trigger condition
  - Throttle conditions
- **Set Alert Actions**: Add a new webhook alert action, by providing the following information:
  - Select **Webhook** as the action.
  - Specify the **URL** to send the JSON payload through an HTTP POST request.
  - (Optional) Provide an **Authorization Header**.
  - (Optional) Provide any **Custom Header**.
  - Enter the **Payload** the webhook will share in JSON format.
  - Select **Trigger for every match** to make a single call for every alert trigger and for the third-party service to send one webhook call for each match in the

results set.

- Click **Save**.

- Click **Save** to finish creating the alert.
- Here's an example of the JSON payload customization:

The user configures an alert for the search query: `eventlog | fields event_time, sourcetype, action, user | limit 10`

You can configure the JSON payload while setting up the webhook connection as follows:

- Option 1: **Trigger for every match** unselected
```
{
    "alert": "My event log alert",
    "time": "{{events[0].event_time}}",          # Get the value of the field 'event_time' from the first record
    "source_type": "{{events[1].sourcetype}}",      # Get the value of the field 'sourcetype' from the second record
    "user": "{{events[2].user}}"                 # Get the value of the field 'user' from the third record
}
```

- Option 2: **Trigger for every match** selected (that is, a separate call per trigger)
```
{
    "alert": "My event log alert",
    "time": "{{event.event_time}}",
    "source_type": "{{event.sourcetype}}",
    "user": "{{event.user}}"
}
```

Forward to Azure

Forward the matched events to an Azure Sentinel instance.

> **Note:** To configure forwarding the matched events to an Azure Sentinel instance, ensure you meet the following prerequisites:
>
> - A Microsoft Entra application used for authentication, with a generated client secret.
> - A Data Collection Endpoint.
> - A custom table in the Log Analytics workspace.
> - A Data Collection Rule (DCR) with a defined alert JSON schema.
> - Permissions that allow the Microsoft Entra application to use the Data Collection Rule.
>
> See the Microsoft documentation for more information about how log ingestion works.
>
> When the alert triggers and Security Analytics sends the alert JSON to Azure, the alert appears in the Azure table. Azure accepts up to 1,000 alerts.
>
> Fields that are absent from the schema are not ingested. If you need to update the schema, update it in Azure and wait for the changes to apply.

> **Note:** DCRs allow you to customize actual field names, data types, and table structures as per the guidelines of your SIEM. Confirm the mappings against active DCR of your organization before final implementation.

Alert Triage

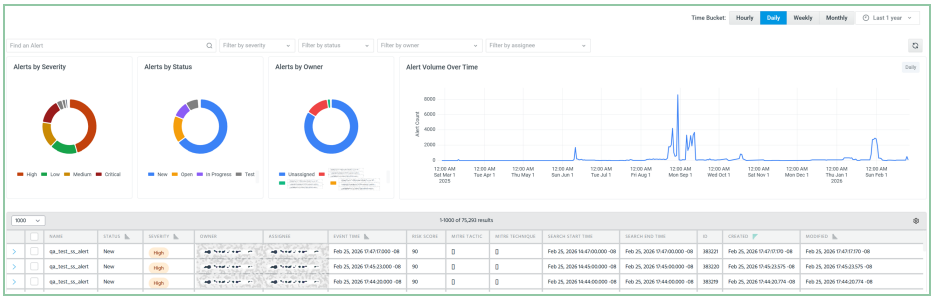
Alert Triage in Anomali Security Analytics helps you investigate, prioritize, and manage triggered alerts.

This centralized workspace provides visualization panels for quick alert assessment and tracking. It also includes tools for filtering, editing, and managing alerts throughout the investigation lifecycle, along with details about MITRE ATT&CK mappings.

While alert rules determine what qualifies as a security event, triage actions define how you interact with those results, including severity assignment, ownership, investigation tracking, and alert management.

> **Note:** Alert Triage data retention is capped at 1 million rows per organization, beyond which the oldest rows will be archived.

(Click the image to enlarge it)



Accessing Alert Triage

To access the **Alert Triage** page, navigate to **Alerting** > **Alert Triage** from the side navigation panel.

Understanding the Interface

The Alert Triage page consists of four main areas:

- **Visualization Panels**: Four panels at the top show alert distribution by severity, status, owner, and volume trends over time.
- **Time Range Controls**: Time bucket selector (**Hourly**, **Daily**, **Weekly**, **Monthly**) and date range picker allow filtering alerts by time period.
- **Filter Controls**: Drop-down filters for severity, status, owner, assignee, along with a text search field help you find specific alerts.
- **Alert Results Table**: A table that displays all alert details including name, status, severity, risk score, MITRE ATT&CK mappings, and entity information.

Alert Triage Workflow

The following workflow helps you effectively triage alerts:

1. **Review Visualization Panels**: Check the severity, status, and volume charts to identify trends and areas requiring immediate attention.

2. **Set Time Range**: Adjust the time bucket and date range to focus on the relevant time period for investigation.
3. **Apply Filters**: Use severity, status, owner, and assignee filters to narrow down the alert list to your focus area.
4. **Select Alerts for Review**: Select an alert in the table and click **Edit** to view detailed information in the **Alert Details** side panel. You can select one or more alerts and configure bulk actions.
5. **Investigate and Update**: Review alert details, MITRE mappings, or entity information, edit alert properties, add comments, or self-assign alerts as needed.
6. **Take Action**: Update alert status or link alerts to new or existing investigations.

Managing Time Range

The time range controls allow you to filter and focus on alerts from specific time periods relevant to your investigation by selecting a time bucket and date range:

- **Time Buckets**: Select **Hourly**, **Daily**, **Weekly**, or **Monthly** to group alert data into time intervals. The default is **Daily**.
- **Date Range**: Use the dropdown to select a preset range (**Last 1 hour**, **Last 2 days**, **Last 7 days**, and more) or specify a custom range. Supports relative time ranges, for example, `now-7d` for the last seven days.

Visualization Panels

You can gain a concise overview of alert distribution and trends through the alert visualization panels:

Panel	Description
Alerts by Severity	Shows alert distribution across severity levels (**Low**, **Medium**, **High**, **Critical**, **Custom**, or **Informational**). Hover over a pie chart segment to see the count. Click the segment to filter the alert table by that severity level.

Panel	Description
Alerts by Status	Displays alerts grouped by status (**New**, **Open**, **In Progress**, **Closed**, or **Custom**). Helps identify alerts requiring attention. Click a pie chart segment to filter the alert table by that status.
Alerts by Owner	Captures alert ownership information by analyst email address. Useful for workload balancing and identifying unassigned alerts. **Note:** See "User Sharing and Permissions" on page 219 for more information on what alerts you can view, edit, clone, or delete.
Alert Volume Over Time	Tracks alert volume trends over the selected time period. Helps identify spikes or patterns in alert generation. Hover over the line chart data points for exact counts.

Alert Results Table

Note: See "User Sharing and Permissions" on page 219 for more information on what alerts you can view, edit, clone, or delete.

The alert results table displays details for all alerts matching your configured filters. The table shows the total number of results and supports pagination for larger result sets.

Column	Description
Name	Displays the alert title or identifier. Select an alert and click **Edit** to open the **Alert Details** side panel.
Status	Shows the current alert status (**New**, **Open**, **In Progress**, **Closed**, or **Custom**). Select an alert and click **Edit** to view or edit the alert status in the Alert Details side panel.

Column	Description
Severity	Denotes the color-coded severity level (**Low**, **Medium**, **High**, **Critical**, **Custom**, or **Informational**). Select an alert and click **Edit** to view or edit the alert severity in the **Alert Details** side panel.
Owner	Captures the email address of the alert creator or analyst who owns this alert. Select an alert and click **Edit** to reconfigure the owner in the **Alert Details** side panel. **Note:** See "User Sharing and Permissions" on page 219 for more information on what alerts you can view, edit, clone, or delete.
Assignee	Denotes the analyst assigned to investigate this alert. New alerts appear as Unassigned until an analyst self-assigns or is assigned by another user.
Event Time	Displays the timestamp when the alert was triggered.
Risk Score	Displays the calculated risk score associated with the alert.
MITRE Tactic	Displays the MITRE ATT&CK tactic associated with this alert (for example, Initial Access, Execution, or Reconnaissance). See the official MITRE ATT&CK documentation for more information.
MITRE Technique	Denotes the specific MITRE ATT&CK technique ID and name describing the adversary behavior, providing detailed context for threat analysis.
Search Start or End Time	Displays the time range for the data that was searched when this alert was generated.
Search Job ID	Job ID of the search
Search Query	AQL query associated with the alert.
ID	ID of the triaged alert.
Created	Timestamp of when the alert was triaged.
Modified	Timestamp of when the triaged alert was modified.

You can also select multiple alerts for bulk operations, such as adding them to new or existing ThreatStream investigations.

Viewing and Editing Alert Details

To edit an alert, select it and click **Edit** in the table to open the **Alert Details** side panel. The panel displays the following information:

- Full alert metadata (name, status, severity, timestamps)
- Risk score
- Comment history with timestamps and analyst names
- Search results of the AQL query associated with the alert, with support for running the query in Search

Editing Alert Properties

Select an alert and click **Edit** in the **Alert Details** panel to edit the following fields:

- **Status**: Update **Status** to **New**, **Open**, **In Progress**, **Custom**, or **Closed**.
- **Severity**: Adjust **Severity** level to ensure the alert is assigned the appropriate risk level.
- **Owner**: Reassign alert ownership to another analyst or team.
- **Assignee**: Assign the alert to yourself or another analyst for investigation.

Adding Comments

Add JIRA-style comments to document your investigation steps, findings, and decisions. Comments are timestamped and include the name of the analyst, creating an auditable history of actions. Multiple comments are supported to facilitate collaboration among team members. You can also edit or delete comments you post.

Self-Assigning Alerts

When you create an alert, it appears as **Unassigned** by default. You can assign the alert to yourself as the Assignee. This enables flexible analyst workload distribution and maintains appropriate alert ownership.

Refresh Alerts

Click **Refresh** ( ) to reload alert data and visualization panels with the latest information. The page does not refresh automatically. Refresh the page to view current data.

Linking to Investigations

You can add one or more alerts to new or existing ThreatStream investigations for comprehensive threat tracking. If you create a new investigation:

1. Enter a name for the investigation.
2. (Optional) Enter a description.
3. Assign the investigation to either a user or a workgroup. By default, it is assigned to you.
4. Set the visibility of the alert to users or workgroups in your organization. By default, it is visible only to you.

> **Note:** See "User Sharing and Permissions" on page 219 for more information on what alerts you can view, edit, clone, or delete.

To add an existing investigation, switch to the **Add to Existing** tab and select an investigation from the drop-down list.

See the ThreatStream Investigation documentation to understand how investigations work.

Managing Alerts

You can edit, clone, or delete alerts that you own. See "User Sharing and Permissions" on page 219 for more information.

Edit an Alert Configuration

To edit an alert:

1. Navigate to **Alerting** > **Manage** > **Alert Rules**.
2. In the **Actions** column, click **Edit** to modify an alert.

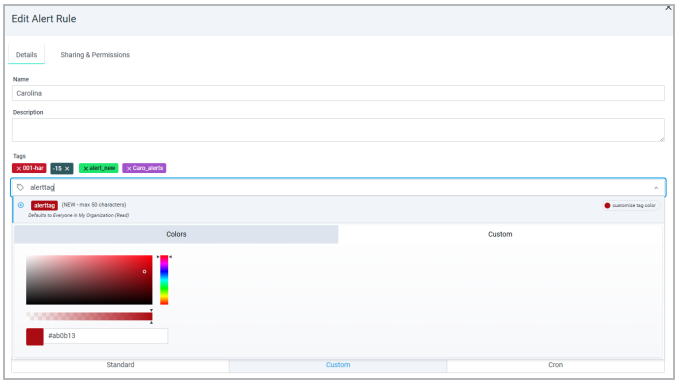
   (Optional) In the **Tags** field:

   a. Enter or select resource tags to apply to the alert. The auto-complete suggestion shows tags you own and tags shared to your organization. Private tags associated with other users are not shown, except to organization administrators.

b. To create a new tag inline, type a name containing up to 50 characters and click **Customize tag color** to select a color. A new tag is added to the shared tag list immediately, even if you abandon updating the alert.

c. To apply an existing tag, type in the field and select it from the auto-complete suggestion results.

d. Click **Manage Resource Tags** to view existing or newly created tags.



3. Click **Save** after making your edits. The changes are applied to the alert.

Newly created tags default to **Everyone in my Organization (Read)**. Only tag owners and users with write permission can add or remove tags. See Resource Tagging Permissions for more information.

Filtering Alerts by Resource Tag

You can filter the alert list by one or more resource tags. When you select multiple tags, only alerts that have all selected tags applied are returned.

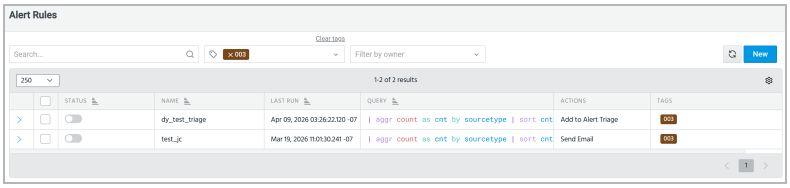
> **Note:** The tag filter drop-down shows only tags you own or that are shared to your organization. Organization administrators can also see private tags owned by other users. See Resource Tagging Permissions for more information.

To filter alerts by resource tag:

1. Navigate to **Alerting** > **Manage** > **Alert Rules**.

2. Click the **Filter by tag** drop-down and select one or more tags. The count displayed next to each tag reflects usage for alerts only, not the total across all

the supported resource types. A tag used across multiple resource types will show a different count on each resource page, depending on the resource you are viewing. The list updates to show only alerts that have all selected tags applied.



3. Click **Clear tags** to clear the filter.

Bulk Editing Tags and Permissions for Alerts

You can add resource tags and update sharing permissions across multiple alerts at once.

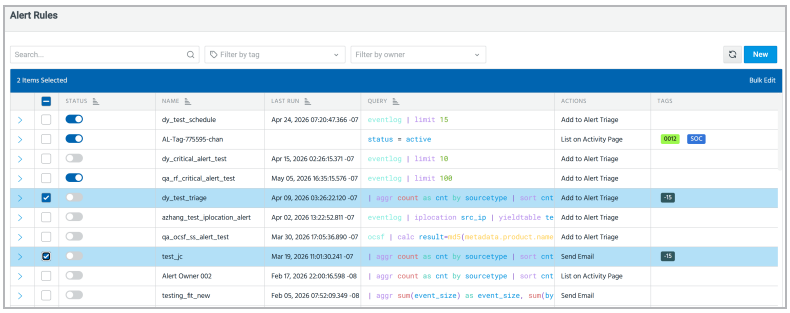
> **Note:** Saving a bulk tag edit replaces the existing tags on all selected alerts. It does not merge with existing tags.

Required Permissions

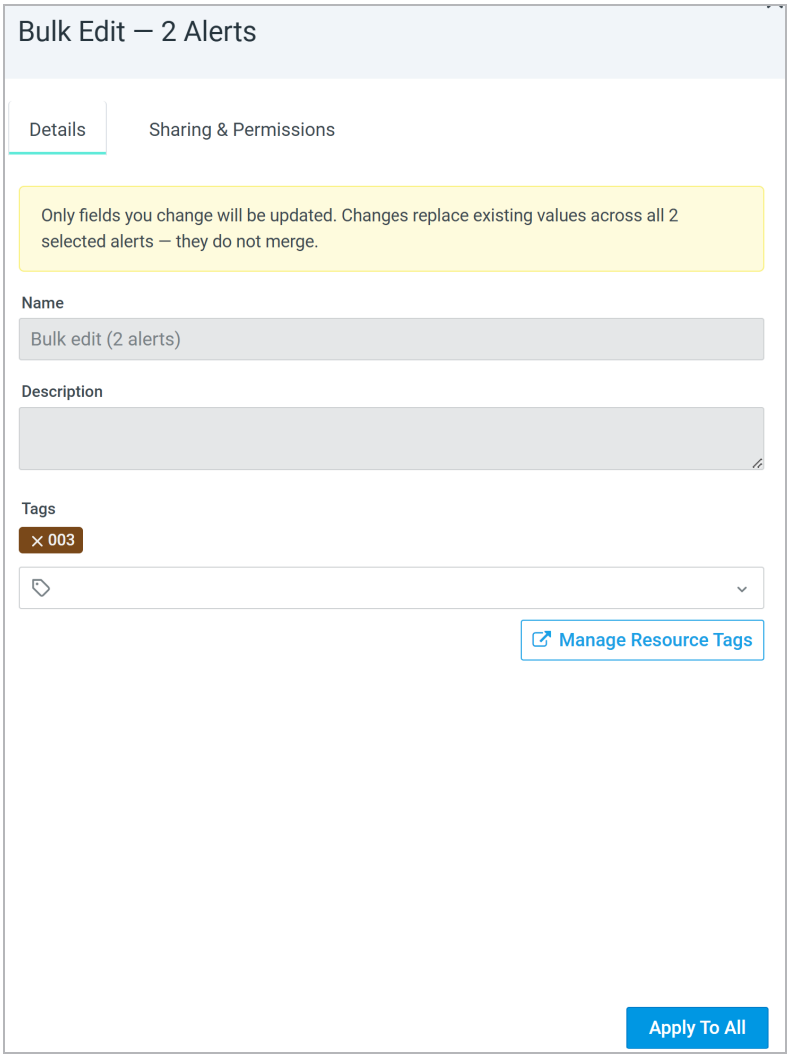
- **Details tab:** Requires write permission or ownership on each selected alert. The tag drop-down shows only tags you own or that are shared to your organization. Organization administrators also see private tags owned by other users.
- **Sharing & Permissions tab:** Available to alert owners and organization administrators only. Users with write-only permission cannot modify sharing settings.

To bulk edit tags and permissions for alerts:

1. Navigate to **Alerting** > **Manage** > **Alert Rules**.
2. Select the alerts you want to update.



3. Click **Bulk edit**.



4. Click the **Details** tab and enter or select tags in the **Tags** field.

5. Enter or select resource tags to apply to the alert. The auto-complete suggestion shows tags you own and tags shared to your organization. Private tags associated with other users are not shown, except to organization administrators.
6. To create a new tag inline, type a name containing up to 50 characters and click **Customize tag color** to select a color. A new tag is added to the shared tag list immediately, even if you abandon updating the alert.
7. To apply an existing tag, type in the field and select it from the auto-complete suggestion results.
8. (Optional) Click the **Sharing & Permissions** tab to update sharing settings for the selected alerts. See Resource Tagging Permissions for more information.
9. Click **Apply to All**.

The tags and permissions are updated for all selected alerts.

Clone an Alert Configuration

	In the **Actions** column, click **Clone** to create an editable copy of an alert.

Delete an Alert Configuration

	In the **Actions** column, click **Delete** to delete an alert.

Managing Saved Searches

> **Caution:** Saved Searches in Security Analytics are deprecated. Please see Saved Searches from AQL Search for more information.

You can use the **Manage** > **Saved Search** page to review the Saved Searches created by you, other users, and administrators.

About Saved Searches

- The Created By column denotes the owner of the saved search.
- The Modified By column denotes the user who modified the saved search. This is either the owner of the saved search or the administrator.
- Administrators are ThreatStream org administrators. Administrators can create, modify, and delete all user-defined saved searches. Non-administrators can modify and delete only the saved searches that they own.

Issue a Saved Search

You can issue a saved search that you created, as well as saved searches created by others.

To run a saved search:

1. Navigate to **Manage** > **Saved Search**.
2. Click the saved search name.

   Search results are shown on the Activity page.

Modify a Saved Search

You can modify the Saved Search configurations that you created but not configurations created by others.

To modify a saved search:

1. Navigate to **Manage** > **Saved Search**.
2. Click the saved search name to issue the search on the Activity Search page.
3. Make your modifications.
4. Save the configuration.

> **Note:** The edits you make to the saved search will impact alerts that reference it.

Delete a Saved Search Configuration

	In the Action column, click the Delete icon to delete a search configuration.

Create an Alert Based on a Saved Search

	In the Action column, click the Alert icon to start the create alert workflow for an alert based on this saved search configuration. See "Using Alerts" on page 215 for complete details on configuring alerts.

Managing Retrospective Search Jobs

You can use the **Manage** > **Retrospective Search** page to view and manage scheduled retrospective search jobs.

About Retrospective Search Jobs

A retrospective search job is a scheduled task to evaluate historic event logs for newly reported indicators of compromise (IOCs). The task repeats on schedule as long as the configuration is active.

Retrospective search job results are written to a CSV file that can be downloaded or emailed to specified email addresses.

Anomali recommends that you schedule retrospective search jobs with settings similar to the following to evaluate IOCs and Threat Model entities that were recently created or modified in ThreatStream.

Search Query	Create separate retrospective search jobs for the key IOCs and Threat Model entities that your security analysts track. You can use ThreatStream search expressions to filter IOCs (called "Observables" in ThreatStream) and Threat Model entities of interest.
Schedule	Every hour
Time Range	Last 1 hour
Event Time Range	Last 6 months

Limitations:

- An organization may configure a maximum of 10 concurrent retrospective search jobs.
- A single search is limited to 100,000 indicators. Therefore, jobs should run on a schedule frequent enough to avoid accumulation of a large number of new or changed indicators within the period specified by Time Range.
- A single Threat Model entity search is limited to 1,000 threat models and a total of 100,000 associated IOCs. Therefore, it is important to use search expression filters to refine your queries for Threat Model entity updates.

Schedule a Retrospective Search Job

You can configure jobs based on search expressions for ThreatStream IOCs or threat model entities.

To create a scheduled Retrospective search:

1. Navigate to **Manage** > **Retrospective Search**.
2. Click **Actions** and select **Schedule Search** at the top right corner.
3. In the Saved Retrospective Search Schedule popup, complete the configuration as described in the following table.

Setting	Description
Name	Type a name that facilitates configuration management. Only ASCII characters are allowed for the configuration name.
Description	A description for the query.

Setting	Description
ThreatStream Search Query	Select a ThreatStream intel category: **IOC**, **Actor**, **Attack Pattern**, **Campaign**, **Threat Bulletin**, **TTP**, or **Vulnerability**. **Note**: The ThreatStream Saved Search or search query you specify must have a search expression that is valid for the ThreatStream intel category you select.
	ThreatStream Saved Search. Click this option and select a ThreatStream saved search to use for the query. For information about creating saved searches in ThreatStream, refer to the following ThreatStream online help topics: ■ Saving Observable Search Filters (IOCs are called Observables in ThreatStream) ■ Saving Threat Model Search Filters (Actor, Attack Pattern, Campaign, Threat Bulletin, TTP, and Vulnerability are among the Threat Model entities in ThreatStream intel)

Setting	Description
	Search query text box. If you do not have a saved search configuration ready to use, you can specify a ThreatStream field-based search expression. For information about ThreatStream search expressions, refer to the following ThreatStream online help topics: ■ Performing Advanced Observable Searches ■ Performing Advanced Threat Model Searches
Time field to use	**Created Timestamp**—Timestamp when the entity was first created on ThreatStream. **Modified Timestamp**—Timestamp when the entity was last modified on ThreatStream.

Setting	Description
Time Range	Specify the time range to constrain the threat intelligence that is used to match against the events. If you selected Created Timestamp earlier, the threat intelligence will be constrained by the timestamp when the threat intelligence *was created* on ThreatStream. If you selected Modified Timestamp earlier, the threat intelligence will be constrained by the timestamp when the threat intelligence *was last modified* on ThreatStream. For example, if you use the default time range of Last 24 hours, this means the threat intelligence created/modified in the last 24 hours will be used to match against the events. If you do not want to use the default time range, click the time picker to specify a new value.
Event Time Range	Specify the time range for the event data that will be searched to match against the threat intelligence constrained by the Search Query and Time Range fields. For example, Last 1 month specifies one month of event data will be searched for the indicator value.

Setting	Description

Schedule	Select a schedule type and define the import schedule:
	■ **Default**: Specify a frequency and start time.
	■ **Cron**: Specify a schedule in cron tab format.
	`# ┌──────────── minute (0 - 59)`
	`# │ ┌──────────── hour (0 - 23)`
	`# │ │ ┌──────────── day of the month (1 - 31)`
	`# │ │ │ ┌──────────── month (1 - 12)`
	`# │ │ │ │ ┌──────────── day of the week (0 - 6) (Sunday to Saturday)`
	`# │ │ │ │ │`
	`# │ │ │ │ │`
	`# │ │ │ │ │`
	`# * * * * *`
	Notes:
	◦ The scheduled time that you configure corresponds with the local time that is read from your Web browser.
	◦ Each organization may configure up to 10 retrospective search jobs. For best performance, Anomali recommends you schedule the jobs to run at different times.

Setting	Description
Run task as	Select a user account to run the scheduled task. Anomali recommends you select a service account for jobs that are a part of your organization's ongoing security practice. A service account is a user account created for the purpose of providing a user and security context to run a service. Typically, a service account is not a human user account.

Setting	Description
Actions	**Enable email delivery** a. Click the **Enable email delivery** option to set up email delivery of the scheduled retrospective search results CSV file. Complete additional settings that become available. b. Enter a single recipient email address or a comma-separated list of email addresses. c. Customize the email subject line and email message text to your preference.

Setting	Description
	Enable Splunk Http Event Collector Specify the following: ▪ **Splunk Host** If your Splunk instance is Splunk Enterprise, specify the fully qualified domain name (FQDN) or IP address for the Splunk host. If your Splunk instance is Splunk Cloud, specify `http-inputs-<host>.splunkcloud.com`, where <host> is the Splunk Cloud Platform instance that runs HEC. For example, `http-inputs-anomali.splunkcloud.com`. Refer to Splunk documentation for more information. ▪ **Splunk Port** Specify the port that is configured in the HTTP Port Number field of Global Settings of Splunk HTTP Event Collector. The default in both Splunk HEC and the Security Analytics alert configuration form is 8088. **Note**: The port for Splunk HEC is typically different from the port for the Splunk dashboard. For example, a Splunk instance can be set up to have the Splunk dashboard accessible at 192.168.10.124:8000 and the Splunk

Setting	Description
Specify the following: ■ **Splunk Host** If your Splunk instance is Splunk Enterprise, specify the fully qualified domain name (FQDN) or IP address for the Splunk host. If your Splunk instance is Splunk Cloud, specify `http-inputs-<host>.splunkcloud.com`, where <host> is the Splunk Cloud Platform instance that runs HEC. For example, `http-inputs-anomali.splunkcloud.com`. Refer to Splunk documentation for more	

4. Click **Save**.

By default, a scheduled Retrospective search is Active—enabled and ready to run at the next scheduled interval. However, you can disable it to prevent it from running.

Toggle Activation for a Retrospective Search Job Configuration

☑	In the Active column, click the checkbox to make the retrospective search job configuration active or inactive.

Modify a Retrospective Search Job Configuration

✎	In the Actions column, click the Edit icon to modify a retrospective search configuration.

Clone a Retrospective Search Job Configuration

⧉	In the Actions column, click the Clone icon to create an editable copy of a configuration.

Delete a Retrospective Search Job Configuration

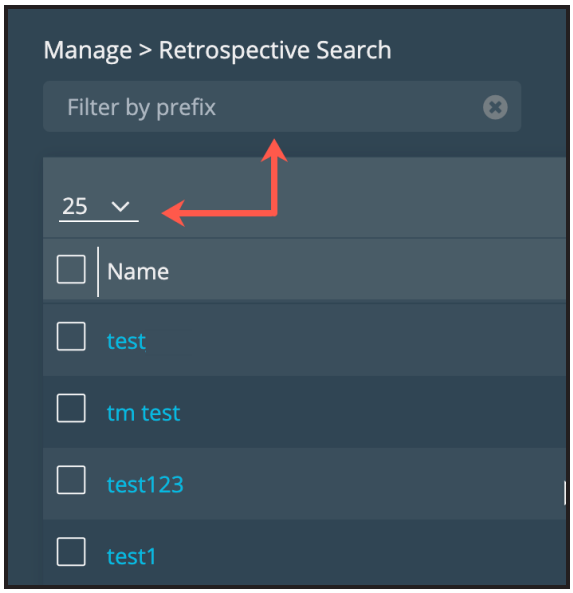
🗑	In the Actions column, click the Delete icon to delete a retrospective search configuration.

View Job History and Download Results

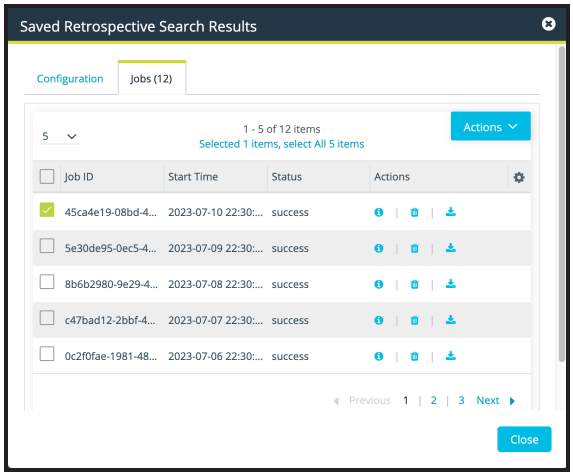
You can view job history and download results from scheduled retrospective search jobs.

To download results:

1. Navigate to **Manage** > **Retrospective Search**.
2. Use the **Filter by prefix** box and page controls to find the name of the configuration you want to examine.



3. Click the hyperlink in the Name column to display the details page.
4. Click the **Jobs** tab.



	In the Actions column, click the Information icon to display job details.
	In the Actions column, click the Delete icon to delete a job result. **To delete multiple results at once:** 1. Select multiple entries in one of the following ways: ▪ Click multiple checkboxes next to the entries. ▪ Click the checkbox in the column heading to select all entries displayed on the tab. 2. Select **Actions** and then click **Delete Selected**.
	In the Actions column, click the Download icon to download a CSV file that contains the results table for the retrospective search job that was run at the time indicated. **Note**: If the Download icon is grayed out, no IOCs were found for the period specified by the job, and there are no results to download.

Troubleshooting

This section describes how to resolve job failures.

Symptom

The scheduled search job history indicates the job failed. The message indicates “Skipped after exceeding the allowed start delay.”

Resolution

Scheduled retrospective search jobs run one at a time. If there are multiple jobs scheduled to run during the same time window, the jobs are queued. Jobs that wait in the queue longer than 10 minutes are purged. Therefore, it is strongly recommended that you stagger the start times for your scheduled retrospective search jobs, and that you avoid scheduling jobs with a frequency that results in potential queuing problems.

Symptom

The scheduled search job history indicates the job failed. The message indicates “Invalid query.”

Resolution

The search failed because the query expression syntax was invalid. Reconfigure the saved search or search query.

For information about ThreatStream search expressions, refer to the following ThreatStream online help topics:

- Performing Advanced Observable Searches
- Performing Advanced Threat Model Searches

Symptom

The scheduled search job history indicates the job failed. The message indicates “Exceeded time limit of 3600 seconds.”

Resolution

The job failed because the query did not send results within the 1 hour limit that is enforced to prevent performance bottlenecks. Consider simplifying your query:

- Try using different filters.
- Reduce the time range for intelligence updates.
- Reduce the event time range.
- Try a combination of these modifications.

Managing Reports

> **Caution:** Reports in Security Analytics are deprecated. Please see Reports from Search for more information.

You can use the **Manage** > **Reports** page to schedule reports. Reports are snapshots of Security Analytics dashboards filtered for a specified time range and search filter expression.

Security Analytics users can view and manage report jobs they created, as well as the report configurations created by others.

Create a Scheduled Report Job

A scheduled report job generates a report that can be downloaded. When you create the scheduled report job, you have the option to set up email notifications with links the recipients can use to download the report.

To create a report job:

1. Navigate to **Manage** > **Reports**.
2. Click **Actions** and select **Schedule Report**.
3. Complete the configuration as described in the following table.

Setting	Description
Name	A meaningful and unique name for the report. This will be used as the report title. The report name can only have letters, numbers, and the underscore, dot, and space characters.
Description	Optional: Describe the purpose of the report.
Report Type	Select one: ■ HTML report ■ PDF report
Dashboard	Select from the following dashboards: ■ Overview ■ Indicator Matches Multi-Dimensional View
Filter	Specify an IOC Match field-based search expression or select an IOC Match saved search to filter data presented in the report.
Time Range	Select a time period, a relative expression, or a date range. The time period filter is based on event time; in other words, the timestamp in the event log.

Schedule	Select a schedule type and define the import schedule:
	■ **Default**: Specify a frequency and start time.
	■ **Cron**: Specify a schedule in cron tab format.
	`# ┌─────────── minute (0 - 59)`
	`# │ ┌─────────── hour (0 - 23)`
	`# │ │ ┌─────────── day of the month (1 - 31)`
	`# │ │ │ ┌─────────── month (1 - 12)`
	`# │ │ │ │ ┌─────────── day of the week (0 - 6) (Sunday to Saturday)`
	`# │ │ │ │ │`
	`# │ │ │ │ │`
	`# │ │ │ │ │`
	`# * * * * *`
	Notes:
	◦ Do not schedule a report job to run more frequently than every 1 hour.
	◦ The scheduled time that you configure corresponds with the local time that is read from your Web browser.

Enable email delivery	**To send the report in an email**: a. Click the **Enable email delivery** option. Complete additional settings that become available. b. Enter a single recipient email address or a comma-separated list of email addresses. c. Customize the email subject line and email message text to your preference.

4. Click **Save**.

   A row for the new scheduled report configuration is added to the report configurations table.

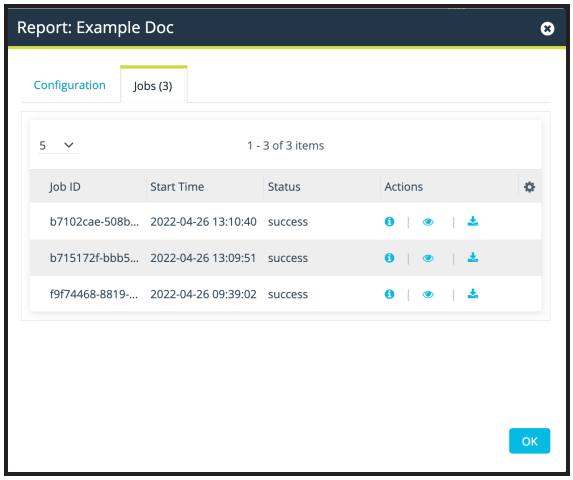
View Report Job History and Download Reports

The scheduled report details page shows a configuration summary and job history. From the job history, you can view information about completed jobs, preview a

particular report, and download a particular report.

To download a report:

1. Navigate to **Manage** > **Reports**.
2. Click the scheduled report configuration name in the first column of the report configurations table to display the details page.
3. Click the **Jobs** tab.



4. Click the Action icons to perform actions described in the following table.

	View job details.
	Preview the report. From the Preview window, you can
	Download the report.

5. Click **OK** to dismiss the detail page and return to the scheduled report configuration list.

Manage Report Configurations

You can edit, delete, preview, or change the active state of a report configuration from the report configurations table.

Preview a Report

	In the Preview column, click the Preview icon. For PDF reports, the preview window has a toolbar you can use to download or print the report preview.

Modify a Report Configuration

	In the Actions column, click the Edit icon.

Delete a Report Configuration

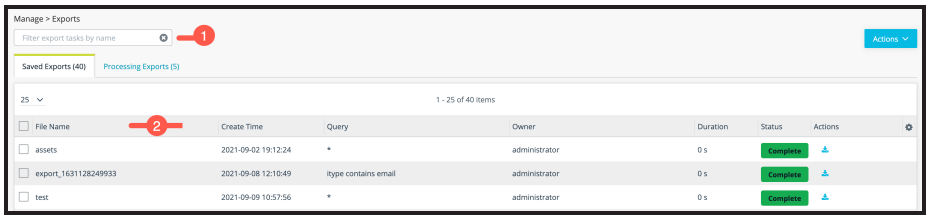
	In the Actions column, click the Delete icon.

Activate/Deactivate a Report Configuration

	In the Active column, toggle the Activation icon. When you toggle the configuration off, the icon is grayed out. The report job associated with the configuration will no longer run on schedule.

Managing Exports

You can use the **Manage** > **Exports** page to view the list of search result export files created by analysts, download them, and delete them.



1	**Filter**: Type text patterns to filter by patterns in the name field.
2	**Sort**: Click column headings to sort the rows in ascending or descending order according to the values in the selected column.

Download an Export

	In the Actions column, click the Download icon to download an export file.

Delete an Export

	In the Actions column, click the Delete icon to delete an export file.

View Export Job Status

Click the **Processing Exports** tab to view the status of incomplete export jobs.

Managing Exclude Lists

You can use the **Manage** > **Exclude List** page to manage exclude lists populated by your analysts.

About Exclude Lists

An *exclude list* is a list of entities (indicator, DGA, asset, IType, feed) that you do not want to examine because they are benign or uninteresting. An exclude list eliminates noise from your research activities.

Once you have added an entity to an exclude list, the search results exclude matches to it from the time it was added. However, any search operations that span the time range *before* the entity was added to the list will still have matches to these entities. Similarly, dashboard widgets that display historical results, such as the Top 20 Impacted Hosts by Risk Score, will continue to show the excluded entity (if it was included *before* being added to the list) until the entity no longer falls into the time range accounted for in the dashboard panel.

Manage the Suppressed Indicators List

The suppressed indicators list includes intelligence indicators that your analysts have marked for exclusion.

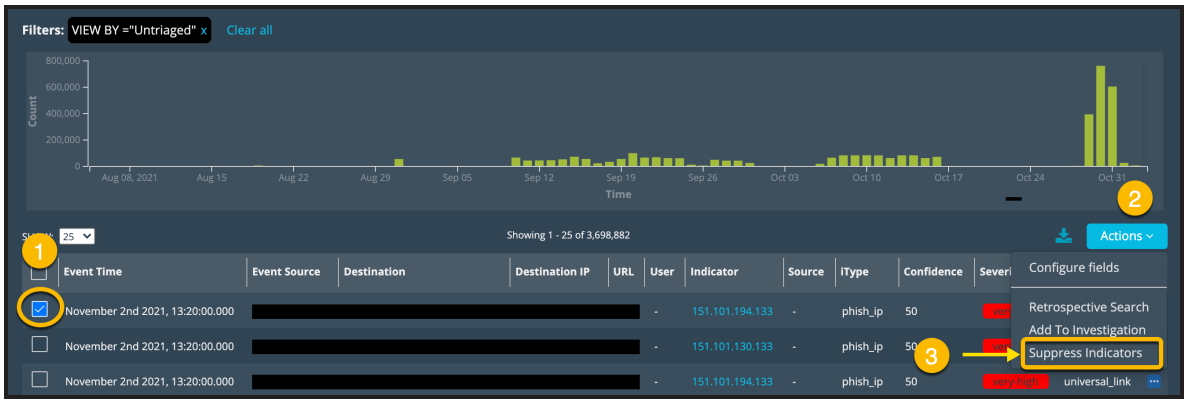
Add Indicators to the Suppressed Indicators List

There are multiple ways analysts can suppress indicators:

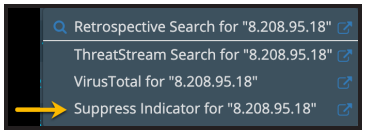
- "Add Indicators from Activity Search Results" below
- "Upload a List of Indicators to Exclude" below

Add Indicators from Activity Search Results

1. From the **Activity** > **IOC Match** results table, select the row or rows for the indicators you want to suppress.
2. Click **Actions** and select **Suppress Indicators**.



Alternatively, you can right-click a value under the Indicator column; and on the context menu, choose **Suppress Indicator for "<*indicator_value*>"** as shown in the following figure.



Upload a List of Indicators to Exclude

Many organizations maintain exclude lists independent from Anomali Security Analytics. You can leverage existing exclude lists by uploading a file or specifying entries manually.

> **Note:** In the file for upload, specify one value per line.

To upload an exclude list:

1. Navigate to **Manage** > **Exclude List**.
2. Click **Actions** and select **Upload**.

3. Select **Suppressed Indicators** as the Content Type.
4. Select **Manual Entry** or **File** as the Upload Type.
5. If your upload type is Manual Entry, enter the suppressed indicator in the **Value** field.

   If your upload type is File, click **Choose File** and browse to the location of your file.
6. Click **Upload**.

The list on the Suppressed Indicators tab is updated.

Remove Indicators from the Suppressed Indicators List

You can delete one entry at a time, multiple entries displayed on the page, or *all* entries on the page.

To remove a single entry:

1. Navigate to **Manage** > **Exclude List**.
2. Click the **Suppressed Indicators** tab.
3. Click the checkbox next to the list entry.
4. Click the delete ( ) icon under the Action column.

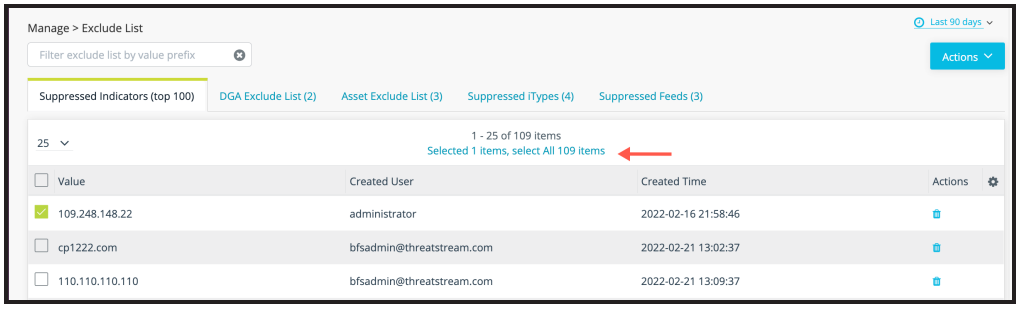
To remove multiple entries from entries displayed on the page:

1. Navigate to **Manage** > **Exclude List**.
2. Select multiple entries in one of the following ways:
   - Click multiple checkboxes next to the entries.
   - Click the checkbox next to the Value column heading to select all entries displayed on the page.
3. Click **Actions** and then select **Remove from List**.

To remove all entries, including those not displayed on the page:

1. Navigate to **Manage** > **Exclude List**.
2. Click the **Suppressed Indicators** tab.

3. Click a checkbox in the Value column and then click the "select all" link below the total number to select all entries, as shown in the following figure.



4. Click **Actions** and then select **Remove from List**.

The list on the Suppressed Indicators tab is updated. Entries removed from the list will be processed again as matched indicators.

Manage the DGA Exclude List

The DGA processor uses two lists to exclude known domains from being processed. The exclude lists define which domains should be considered benign and excluded from the DGA determination process. One of these exclude lists is maintained by Anomali. It is based on millions of well-known domains, such as microsoft.com, google.com, and so on. The second exclude list is maintained by your organization.

> **Note:** You can specify up to 10,000 domains.

Add Domains to the Exclude List

Analysts can add any domains in the following ways:

- From the **Activity** > **DGA Match** search results table, select a row or rows, click **Action** and select **Mark as False Positive**.
- Upload a file or manually enter domains to exclude.

> **Note:** In the file for upload, specify one DGA entry per line.

To add domains to the DGA exclude list:

1. Navigate to **Manage** > **Exclude List**.
2. Click **Actions** and then select **Upload**.
3. Select **DGA Exclude List** as the Content Type.
4. Select **Manual Entry** or **File** as the Upload Type.
5. If your upload type is Manual Entry, enter the domain in the **Value** field.

   If your upload type is File, click **Choose File** and browse to the location of your file.
6. Click **Upload**.

The list on the DGA Exclude List tab is updated.

Remove Domains from the Exclude List

You can delete one entry at a time, multiple items displayed on the page, or *all* items on the page.

To remove a single entry:

1. Navigate to **Manage** > **Exclude List**.
2. Click the **DGA Exclude List** tab.
3. Click the checkbox next to the list entry.
4. Click the delete ( ) icon under the Action column.

To remove multiple entries from entries displayed on the page:

1. Navigate to **Manage** > **Exclude List**.
2. Click the **DGA Exclude List** tab.
3. Select multiple entries in one of the following ways:
   - Click multiple checkboxes next to the entries.
   - Click the checkbox next to the Value column heading to select all entries displayed on the page.
4. Click **Actions** and then select **Remove from List**.

To remove all entries, including those not displayed on the page:

1. Navigate to **Manage** > **Exclude List**.
2. Click the **DGA Exclude List** tab.
3. Click a checkbox in the Value column and then click the "select all" link below the total number to select all entries.
4. Click **Actions** and then select **Remove from List**.

The list on the DGA Exclude List tab is updated. Entries removed from the list will be processed again as DGAs.

Manage the Asset Exclude List

If an asset is incorrectly matched or you want to stop a matched asset from being matched again, you can add it to an asset exclude list. Assets on the list are excluded from the asset matching process.

Add Entries to the Exclude List

Analysts can add any domains in the following ways:

- From the **Activity** > **Asset** search results table, select a row or rows, click **Action** and select **Add selected asset to exclude list**.
- Manually enter asset details.

To add manual entries:

1. Navigate to **Manage** > **Exclude List**.
2. Click the **Asset Exclude List** tab.
3. Click **Actions** and then select **Upload**.
4. Enter the asset IP address. To specify an IP address range, use CIDR format (for example, `192.0.2.0/24`).
5. Optional. Enter a description, location, and department.
6. Click **Upload**.

The asset is added to the list.

Remove Entries from the Exclude List

You can delete one entry at a time, multiple entries displayed on the page, or *all* entries on the page.

To remove a single entry:

1. Navigate to **Manage** > **Exclude List**.
2. Click the **Asset Exclude List** tab.
3. Click the checkbox next to the list entry.
4. Click the delete ( ) icon under the Action column.

To remove multiple entries from entries displayed on the page:

1. Navigate to **Manage** > **Exclude List**.
2. Click the **Asset Exclude List** tab.
3. Select multiple entries in one of the following ways:
   - Click multiple checkboxes next to the entries.
   - Click the checkbox next to the IP/IP Ranges column heading to select all entries displayed on the page.
4. Click **Actions** and then select **Remove from List**.

To remove all entries, including those not displayed on the page:

1. Navigate to **Manage** > **Exclude List**.
2. Click the **Asset Exclude List** tab.
3. Click a checkbox in the IP/IP Ranges column and then click the "select all" link below the total number to select all entries.
4. Click **Actions** and then select **Remove from List**.

The list is updated.

Manage the Suppressed iTypes List

You can suppress correlation with specific iTypes if you find you are categorically not interested in them.

Add Entries to the Suppressed iTypes List

Analysts can add iTypes to the list in the following ways:

- From the Match Analysis Dashboard | Matches by iType table. Right-click an iType and select **Suppress this itype**.
- Manually enter the iType.

To add manual entries:

1. Navigate to **Manage** > **Exclude List**.
2. Click **Actions** and then select **Upload**.
3. Select **Suppressed iTypes** as the Content Type.
4. Type the iType name and then click the + icon. You can repeat this to add more than one-at-time.
   Note: The name must match the iType name exactly. Refer to "ThreatStream Indicator Types" on page 1028 for a list of iType names.
5. Click **Upload**.

The iType is added to the list.

Remove Entries from the Suppressed iTypes List

You can delete one entry at a time, multiple entries displayed on the page, or *all* entries on the page.

To remove a single entry:

1. Navigate to **Manage** > **Exclude List**.
2. Click the **Suppressed iTypes** tab.
3. Click the checkbox next to the list entry.
4. Click the delete ( ) icon under the Action column.

To remove multiple entries from entries displayed on the page:

1. Navigate to **Manage** > **Exclude List**.
2. Click the **Suppressed iTypes** tab.
3. Select multiple entries in one of the following ways:

- Click multiple checkboxes next to the entries.
- Click the checkbox next to the Value column heading to select all entries displayed on the page.

4. Click **Actions** and then select **Remove from List**.

To remove all entries, including those not displayed on the page:

1. Navigate to **Manage** > **Exclude List**.
2. Click the **Suppressed iTypes** tab.
3. Click a checkbox in the Value column and then click the "select all" link below the total number to select all entries.
4. Click **Actions** and then select **Remove from List**.

The list is updated.

Manage the Suppressed Feeds List

You can suppress correlation with specific intelligence feeds if you find you are categorically not interested in them.

Add Entries to the Suppressed Feeds List

Analysts can add feeds to the list in the following ways:

- From the Match Analysis Dashboard | Matches by Feed table. Right-click a feed ID and select **Suppress this feed**.
- Manually enter the feed ID.

To add manual entries:

1. Navigate to **Manage** > **Exclude List**.
2. Click **Actions** and then select **Upload**.
3. Select **Suppressed Feeds** as the Content Type.
4. Type the feed ID and then click the + icon. You can repeat this to add more than one-at-time.
   Note: The values you specify must match the ThreatStream feed ID exactly.
5. Click **Upload**.

The feed is added to the list.

Remove Entries from the Suppressed Feeds List

You can delete one entry at a time, multiple entries displayed on the page, or *all* entries on the page.

To remove a single entry:

1. Navigate to **Manage** > **Exclude List**.
2. Click the **Suppressed Feeds** tab.
3. Click the checkbox next to the list entry.
4. Click the delete ( ) icon under the Action column.

To remove multiple entries from entries displayed on the page:

1. Navigate to **Manage** > **Exclude List**.
2. Click the **Suppressed Feeds** tab.
3. Select multiple entries in one of the following ways:
   - Click multiple checkboxes next to the entries.
   - Click the checkbox next to the Value column heading to select all entries displayed on the page.
4. Click **Actions** and then select **Remove from List**.

To remove all entries, including those not displayed on the page:

1. Navigate to **Manage** > **Exclude List**.
2. Click the **Suppressed Feeds** tab.
3. Click a checkbox in the Value column and then click the "select all" link below the total number to select all entries.
4. Click **Actions** and then select **Remove from List**.

The list is updated.

Managing Lookup Tables

> Management of lookup tables within Security Analytics is soon to be deprecated. To create and manage lookup tables, you will have to use the Search menu. Refer to Managing Lookup Tables for details.
> If you have questions about this change, contact Anomali Customer Support.

You can use the **Manage** > **Lookup Table** page to upload, view, append, update, export, or delete lookup tables used in Search.

Lookup Table Permissions

- All users can upload lookup tables.
- All users can use Search to query any lookup table.
- Non-Org Admin users can append, update, and delete only lookup tables they own.
- Org Admin users can append, update, and delete any lookup table.

About Lookup Tables

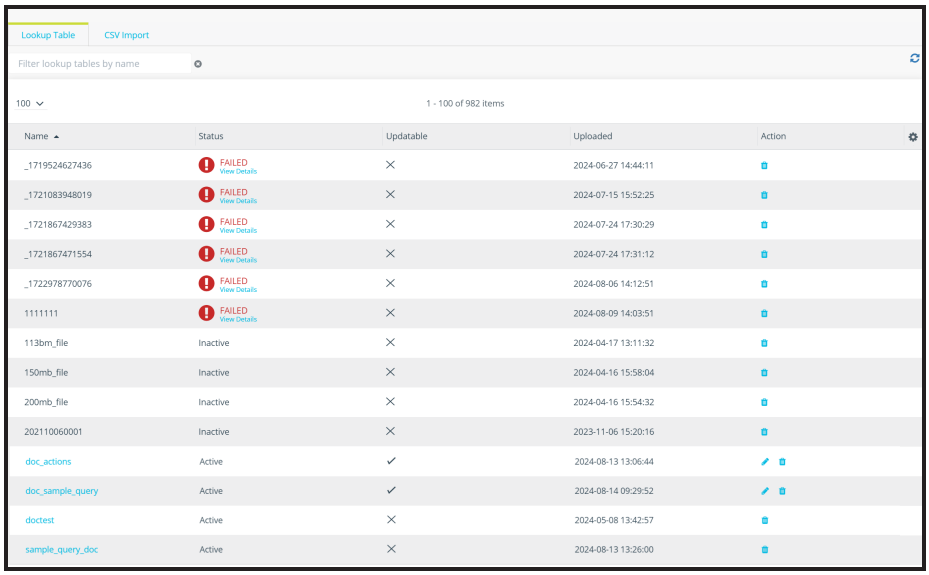
A *lookup table* is a CSV file that has enrichment data—for example, the commonly used MaxMind IP geolocation data. A lookup table can be any set of fields that you want to correlate with an event log field, enabling the lookup table data to enrich Search results.

From the **Manage** > **Lookup Table** page, you can perform the following actions:

- Upload a lookup table
- View a lookup table
- Append to an existing lookup table
- Update a lookup table

- Export a lookup table
- Delete a lookup table

You cannot activate a lookup table. Active and inactive statuses are reported on the Lookup Table tab of the Lookup Table page. An active status indicates that the table has been created and is ready to be used in AQL Search. An inactive status indicates that activation is not yet completed. If there is a problem with the table validation, the failed status is displayed. To know the reason the lookup table activation failed, click **View Details** next to the Failed status.



Upload a Lookup Table

You can add a lookup table to your AQL Search environment by uploading a comma-separated value (CSV) file. Additionally, you can add values to existing lookup tables.

CSV Import Guidelines

To successfully upload a lookup table, follow these file upload guidelines:

- The upload file must have a heading row with the lookup table field names.
- Avoid using the same field names as the eventlog schema.

- In searches, field name is case sensitive, so use capitalization conventions that are easy for search users to follow. For example, all lowercase.
- Enclose values that have spaces in straight quotation marks (").
- File formats must be CSV, .gz, or .tar.
- The upload file can be a maximum of 100 MB.

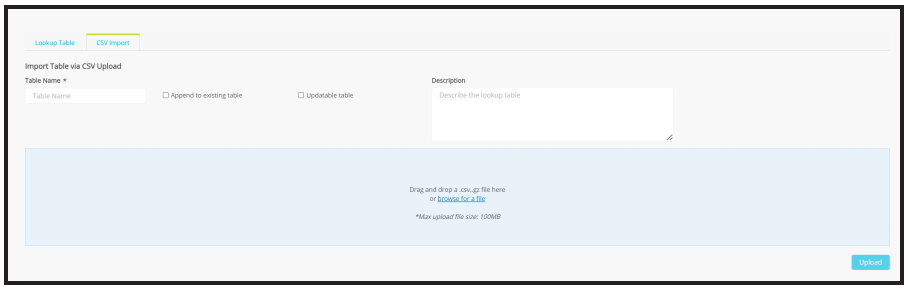
> **Note:**
> If your CSV file is larger than 100 MB, use the following guidelines to upload your data:
>
> - Compress the file to reduce its size.
> - Split the content into multiple smaller files. After that, upload the first file to create a lookup table and append the remaining files to this table. See "Append to an Existing Lookup Table" on page 287 for more information.

The following is an example of a lookup table:

	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					

To upload a lookup table:

1. Create a CSV file that contains the required values, as described above.
2. Navigate to **Manage** > **Lookup Table**.
3. Click the **CSV Import** tab.



4. Specify a name in the **Table Name** box.

> **Note:**
> - This is the lookup table name that users can reference in AQL Search.
> - The name may contain only alphanumeric characters and underscores.
> - The name cannot begin with a number.
> - Do not name the table the same name as an event field or lookup table field.

5. (Optionally) Select **Append to existing table** if you want to add the rows to an existing lookup table. See "Append to an Existing Lookup Table" on the next page for details.

6. (Optionally) Select **Updatable table** if you want to be able to make updates to the table. See "Update a Lookup Table" on page 288 for details.

> **Note:** System tables and lookup tables created using the `yieldtable` operator cannot be updated.

7. (Optionally) Enter a description of the lookup table in the Description box.

8. Use the file controls to browse and select your CSV file.

9. Click **Upload**.

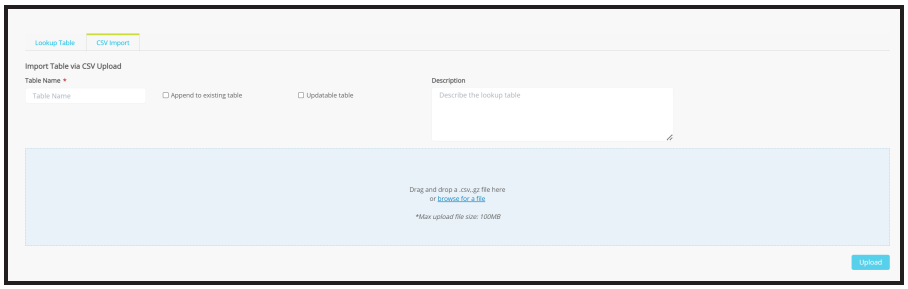
The lookup table is added to the list of lookup tables on the Lookup Table tab.

Append to an Existing Lookup Table

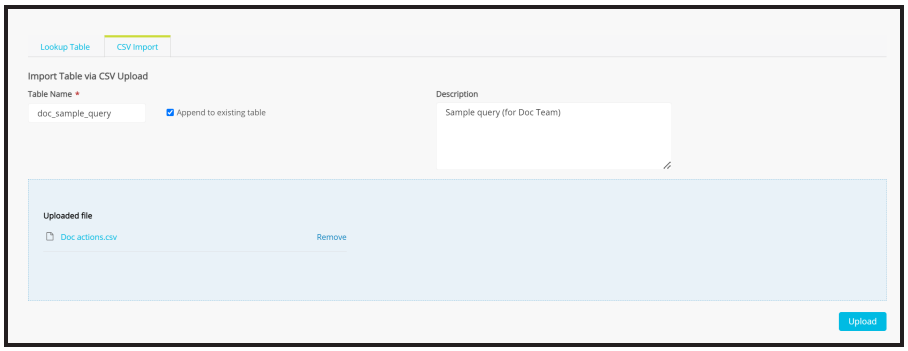
> **Note:** This feature only enables you to add rows in bulk to an existing lookup table. To delete rows in an existing non-updatable lookup table, you must delete the table and upload a new table with the rows you need. To add, edit, or delete rows in an updatable lookup table, use the update feature ( ) on the Lookup Table tab. Refer to "Update a Lookup Table" on the next page for details.

To append (add rows in bulk) to an existing lookup table:

1. Create a CSV file that contains the rows you want to add to an existing lookup table.
2. Navigate to **Manage** > **Lookup Table**.
3. Click the **CSV Import** tab.



4. In the **Table Name** box, specify the name of the lookup table to which you want to add rows.
5. Click **Append to existing table**. Note that the rows you add must have the same number of columns as the lookup table to which you add the rows.
6. (Optionally) Enter a description of the lookup table in the Description box.
7. Use the file controls to browse and select your CSV file.



8. Click **Upload**.

The rows are added to the existing lookup table.

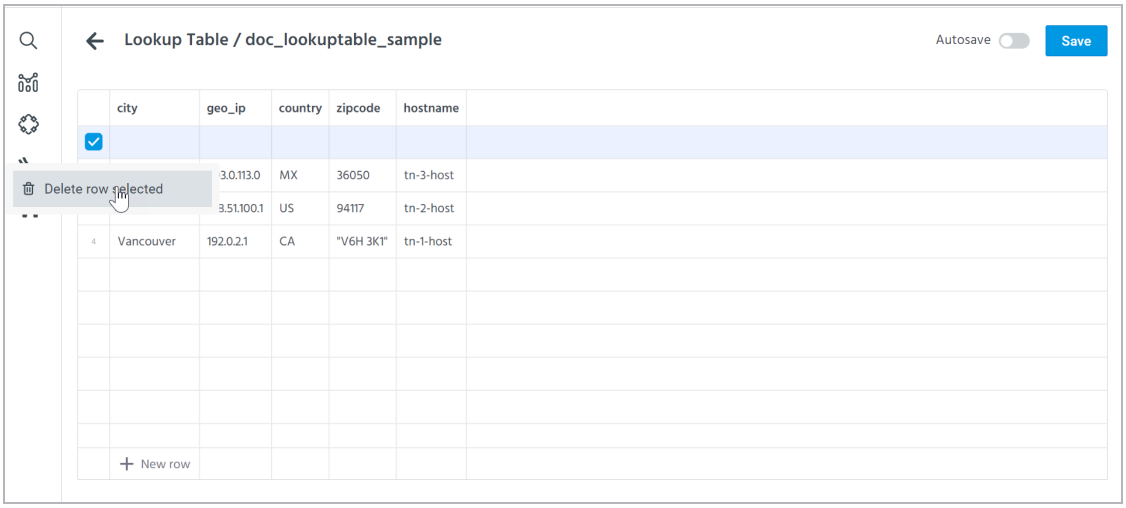
Update a Lookup Table

Updatable lookup tables can be modified. You can edit cell values, add rows, and delete rows.

To update a lookup table:

1. Navigate to **Manage** > **Lookup Table**.

2. Click the edit icon ( ) corresponding with the lookup table you want to update. You are redirected to the table in the edit mode.



3. (Optionally) Enable **Autosave** to automatically save your updates. Updates are autosaved every minute.

4. Modify the lookup table:
   - To add a new row to the table, click **+ New row**.
   - To delete a row, select the row you want to delete, right click on the selected row, and click **Delete row selected**.
     To delete all rows, select the header row, right click on the rows, and click **Delete rows 1-x**.
   - To edit a cell value, double click on a cell and edit its value. Values in the header row cannot be modified.
5. Click **Save**.

The lookup table is updated.

View a Lookup Table

To view a lookup table:

1. Navigate to **Manage** > **Lookup Table**.
2. Click the active lookup table of interest.

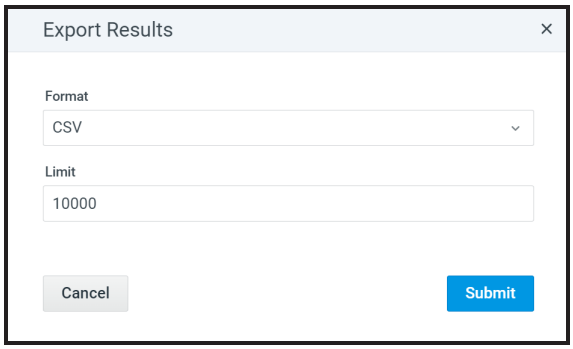
You are redirected to the Result tab of the AQL Search page.

Export a Lookup Table

To export a lookup table:

1. Navigate to **Manage** > **Lookup Table**.
2. Click the active lookup table of interest. You are redirected to the Result tab of the AQL Search page.
3. Click the Export icon ( ).

4. In the Export Results dialog box, select an export format (CSV or JSON) and enter a maximum number of rows you want to export.



5. Click **Submit**.

Downloading of the lookup table starts immediately.

Delete a Lookup Table

To delete a lookup table:

1. Navigate to **Manage** > **Lookup Table**.
2. In the Action column, click the Delete icon ( ) corresponding with the lookup table you want to delete.

The lookup table is deleted.

Chapter 5: Modifying My Profile

You can use the My Profile page to change settings related to your user account. Changes you make to your profile do not affect other users.

Change the Default Date Range Filter

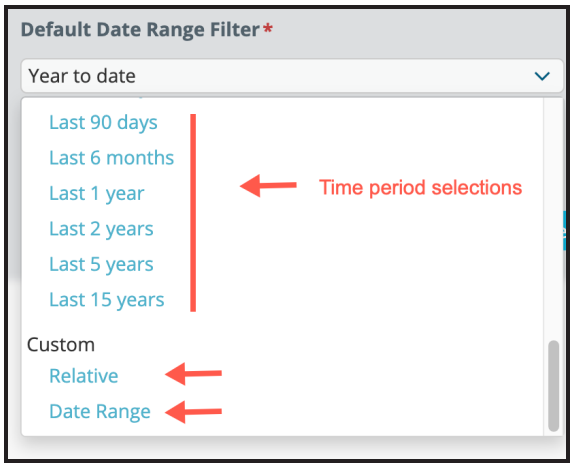
Anomali Security Analytics Dashboard panels and Activity searches display results for a specified time period. You can configure a global default associated with your user account. On each page, there are time range controls you can use to examine results from different time periods.

Notes:

- The default date range filter specified in My Profile settings determines only what the behavior is if you do not specify a time range on the Dashboard and Activity pages.
- If you specify a different time period on those pages, that time period persists across the Dashboard and Activity search pages for the duration of your browser session or until you specify a different time period.
- When you open a new browser session and authenticate again, the default specified in My Profile settings is applied and persists until you specify a different time period on a Dashboard or Activity search page.

To change the default:

1. Click the profile icon in the left navigation panel and select **My Profile**.
2. Use the **Default Date Range Filter** controls to select a time period, a relative expression, or a date range.


Default Date Range Filter*
Year to date
Last 90 days
Last 6 months
Last 1 year
Last 2 years
Last 5 years
Last 15 years
Time period selections
Custom
Relative
Date Range

3. Click **Save**.

Chapter 6: Managing Anomali Security Analytics Settings

Administrators are responsible for creating and modifying Security Analytics platform settings and Security Analytics integration settings, and for deleting them when it is appropriate.

You must have the ThreatStream **Org Admin** permission to view and use the Security Analytics Settings menu. For information about the **Org Admin** permission, see the ThreatStream online help.

You can use the Settings menu to perform the following activities:

- Onboard Links and event log sources
- Import asset data from scanner reports or CSV files
- Create alerts
- Tune DGA match, iType filter, asset field, event field, and correlation engine settings

Configuring General Settings

You can use the **Settings** > **General Settings** page to modify default settings or add custom fields. Typically, you make changes to General Settings only if your IT environment has special requirements.

Modify DGA Settings

DGA settings can be used to tune matching for the DGA match index. Typically, you do not need to adjust or tune these settings. Do so only as directed by Anomali Customer Support.

To modify DGA settings:

1. Click the Settings icon in the left navigation panel and select **Security Analytics**.

2. Click **General**.
3. Click the **DGA Settings** tab.

Setting	Description
Threshold	Defines the threshold probability a domain is generated by a DGA. Domains determined less likely to be DGA domains than this threshold are considered benign and are not matched. The probability is calculated using machine-learning algorithms. Default: 0.6 (or 60%). Valid values for this field are between 0 and 1.
Batch Size	Defines the number of events that are processed for DGA determination per batch. The default value, 10000, is an optimal size for most environments. Do not change it unless directed by Customer Support.

4. Click **Save**.

> **Note:** The configuration changes take effect immediately but do not change matches that have already been recorded.

Modify Filter Settings

Filter settings can be used to tune matching for the IOC match index. By default, event correlation is performed against all ThreatStream indicators from all feeds that your organization has subscribed to, regardless of an indicator's severity, confidence, or any other enrichment data associated with it.

If desired, you can define a filter to correlate events with ThreatStream indicators that meet the criteria specified by the filter. For example, you can define a filter that correlates against indicators with `confidence >= 90 AND severity = "very-high"`.

To modify filter settings:

1. Click the Settings icon in the left navigation panel and select **Security Analytics**.
2. Click **General**.
3. Click the **Filter** tab.
4. Configure a filter expression. See the sections that follow this procedure for details on the filter fields and operators you can use to specify filter expressions.
5. Click **Save**.

> **Note:** The configuration changes take effect immediately but do not change matches that have already been recorded. In searches for periods before the setting was changed, you will still observe matches for IOCs that were not excluded when event logs for earlier periods were ingested.

Filter Examples

The following are a few example filters:

```
classification = "private"
source_feed_id = 678
itype contains "domain"
srcip startswith "192."
domain endswith ".net"
country='US' OR country = 'CH' or country = 'JP'
confidence>=75 AND (severity = 'high' or severity = 'very-high')
AND country != 'US'
confidence >70 and (type != email AND type != md5)
( confidence > 70 ) AND (itype=mal_domain OR itype=mal_ip OR
itype=c2_domain OR itype=c2_ip OR itype=apt_domain OR itype=apt_ip
OR itype=exploit_ip OR itype=exploit_domain )
```

Filter Operators

The following table describes the logical operators you can use to form complex field-based search expressions. Operator names are **not** case sensitive.

Field Type	Use this Operator
String	=, !=, contains, startswith
Numeric	=, !=, <, <=, >, >=
Date	=, !=, <, <=, >, >=
Logical	AND, OR, NOT, (*specify a parenthetical expression*)

Filter Fields

The following table describes the fields that can be used in filter expressions.

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: private, public **Notes:** - Private also includes Trusted Circles. - `classification` is displayed as Visibility on the ThreatStream user interface.
confidence	Numeric	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: *YYYY-MM-DD***T***hh:mm:ss*, where T denotes the start of the value for time. For example, 2014-10-02T20:44:35. • 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.
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.
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.

Field Name	Type	Description
is_osint	Boolean	Whether the observable is from an open source intelligence feed.
itype	String	Indicator type. For example, c2_ip, compromised_email, apt_md5, and so on. See "ThreatStream Indicator Types" on page 1028 for a complete list.
lat	Numeric	Latitude associated with the Geo location of the IP.
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: *YYYY-MM-DD***T***hh:mm:ss*, where T denotes the start of the value for time. For example, modified_ts > 2014-10-02T20:44:35. • 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. The following example shows how you will use this field in a filter: modified_ts > -14d.
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.

Field Name	Type	Description
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.
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.

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 score from 0 to 100, provided by the source of the observable.
stream_id	Numeric	ID of the threat feed that created the observable on ThreatStream.
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
tags	String	Additional comments and context associated with the observable when it was imported from its original threat feed. **Note:** • The correlation filter is case sensitive. For example, the expression `tags="log4j"` and `tags="Log4j` produce different, case-sensitive results.
threat_type	String	Summarized threat type of the observable. For example, malware, compromised, apt, c2, and so on.
tlp	String	Traffic Light Protocol designation for the observable—red, amber, green, white.

Field Name	Type	Description
trusted_circle_id	String	ID of the trusted circle with which the observable is shared.
type	String	Data type of the observable. Possible values: ip, domain, url, email, md5
value	String	Specifies the value of an observable, whose type is specified by the "type" field.

Modify My Data Settings

Anomali Security Analytics would like your permission to collect usage and diagnostic data. Enabling the data collection will help improve Anomali Security Analytics.

By default, data collection is enabled, and data collection begins when users in your organization log in.

To change the data collection setting:

> **Note:** If data collection is currently enabled and now you want to stop it, notify your users because their current sessions will be terminated momentarily, and they will be redirected to the login page.

1. Click the Settings icon in the left navigation panel and select **Security Analytics**.
2. Click **General**.
3. Click the **My Data** tab.
4. Click the slider to enable or disable the data collection.
5. Click **Save**. The following message is displayed for the setting to disable:
6. Review the message and confirm by clicking **Yes**.

If you changed from enabled to **disabled**, all active sessions will be terminated momentarily. Users will then be redirected to the Anomali Security Analytics login page.

If you changed from disabled to **enabled**, user sessions will not be disrupted. Data collection will take effect when the user logs back in.

Managing Links and Log Sources

You use the **Settings** > **Links** page to monitor the health of Anomali Links and to configure log sources.

> **Note:**
> - You can add use the Security Analytics user interface to add log sources and manage active/inactive status for on-prem-to-cloud data flows through Universal Link.
> - Anomali Customer Support will facilitate the onboarding and management of log sources for cloud-to-cloud data flows.

About Links

Anomali Link software is not required for all log sources. In cases where Link software is required, Anomali maintains and supports Anomali Link software to perform the following functions:

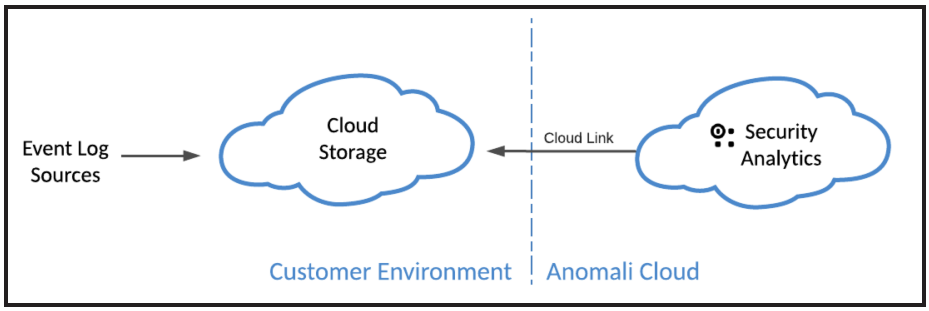
- Collect data from the event source
- Parse the data into normalized event log fields
- Upload the normalized event log data to Security Analytics

Cloud-to-Cloud Data Flow Using Anomali Cloud Link

Anomali Cloud Link ingests event telemetry that has been forwarded to cloud storage, such as Amazon Web Services S3, Microsoft Azure Event Hub, or Google Cloud Storage. For these types, Security Analytics initiates queries to retrieve logs.

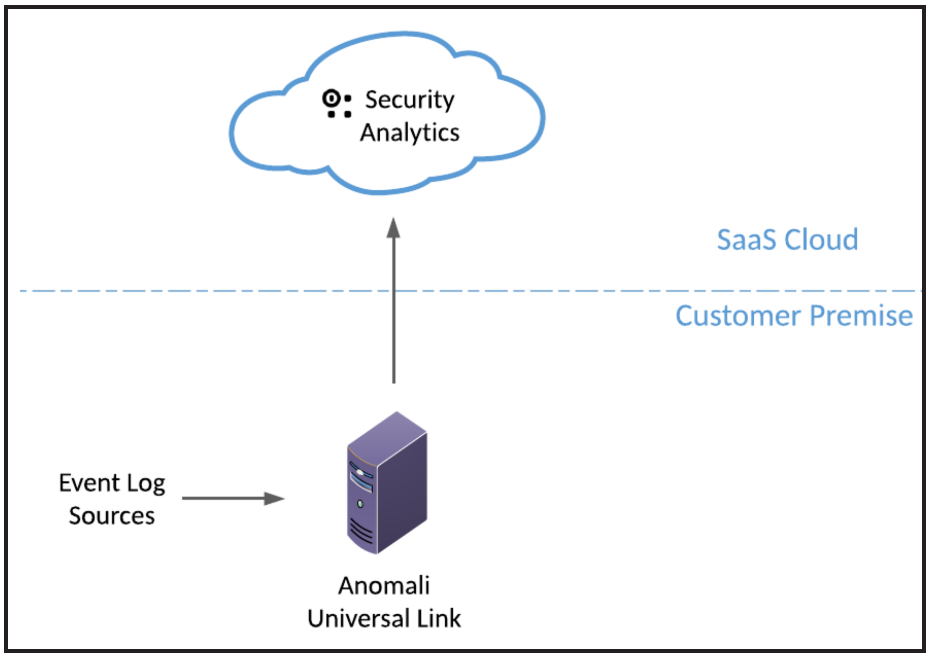
For live streamed events, the process is automatic once set up and does not require any intervention from you.

For backfilling events that are older than 24 hours from now, you must contact Anomali to set up ingestion for your organization. Failing to do so can result in an impact on the timestamps of those events thus leading to inaccurate search and correlation results.



On-Premise-to-Cloud Data Flow Using Anomali Universal Link

For on premise log sources, @Anomali software is deployed on the SIEM system or on another system in your local network. A Universal Link instance connects to Security Analytics on one side and to a SIEM (or other event source) on the other side.

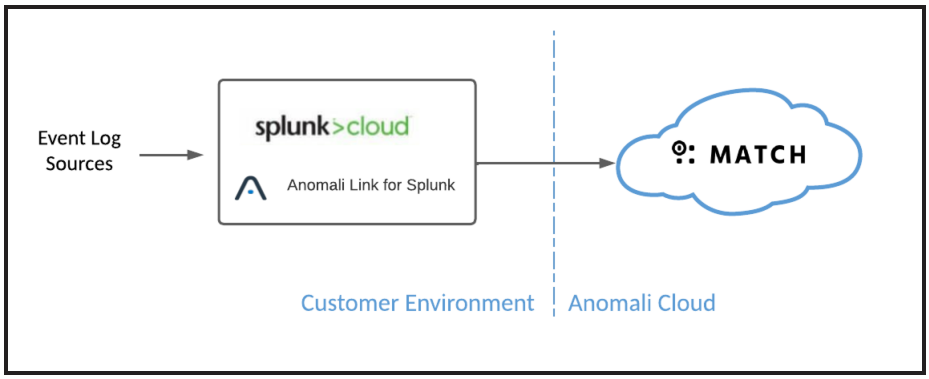


For information about installing Anomali Universal Link in your on premise environment, see the *Anomali Universal Link Installation Guide*.

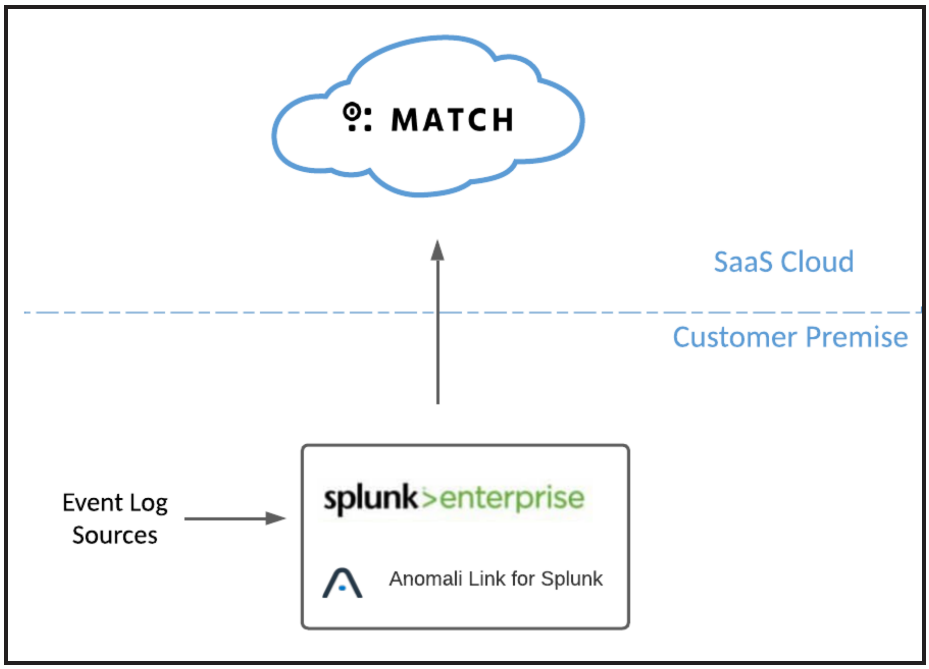
Anomali Link for Splunk

For log ingestion from Splunk, Anomali Link for Splunk is deployed on Splunk Cloud or Splunk Enterprise to facilitate log forwarding to Security Analytics.

The following figure shows a deployment with Splunk Cloud.



The following figure shows a deployment with Splunk Enterprise.



For information about installing Anomali Link for Splunk, see *Anomali Link (for Splunk) Installation Guide*.

Monitor Link Health

The Link Summary page displays health indicators for Universal Link and Splunk Link instances. The Link Details page displays health indicators for the log sources configured for the Link.

> **Note:** Cloud Link instances are monitored by Anomali. If desired, you can confirm logs are

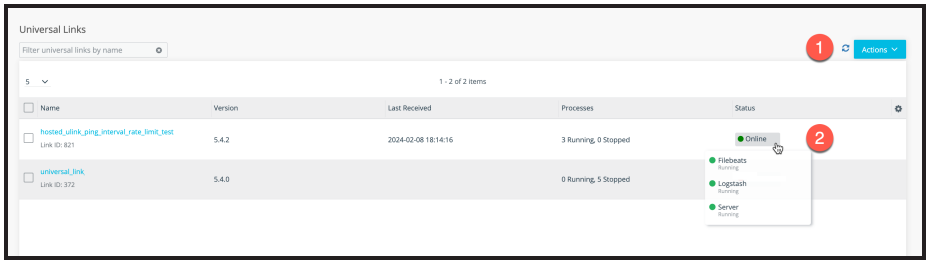
being ingested by issuing a search similar to the following natural language query in AQL search:

```
-- latest crowdstrike logs
```

See Getting Started with AQL Search in the AQL Search Help Center to learn about AQL search.

Link Summary Page

The Link Summary page shows version information, a timestamp for the last data received, process status, and online status. The following figure shows the Link Summary page for a Universal Link instance.

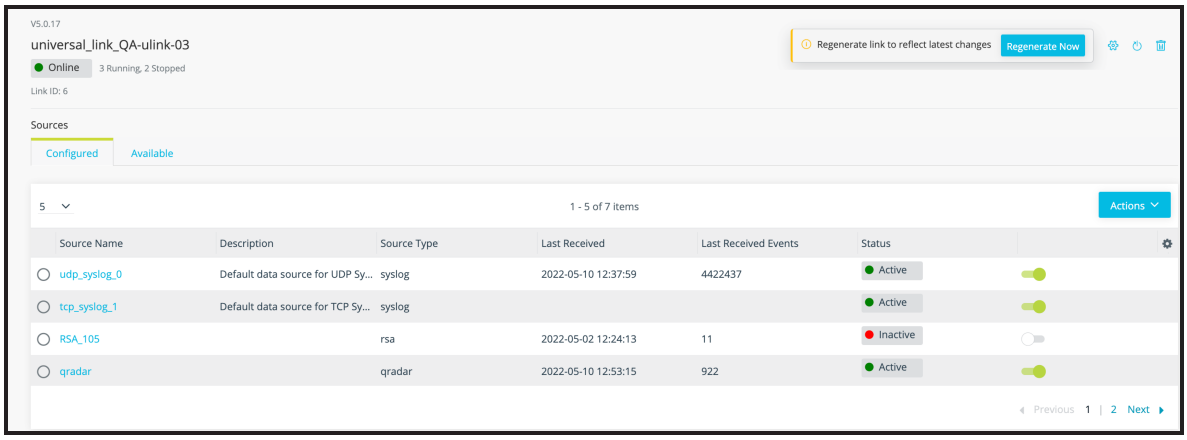


1	**Refresh:** Click the Refresh icon (⟲) to send health status queries again.
2	**Process status**: Mouse over the Status icon to display process status details. Restart the Link if a process is stopped when it is expected to be running. See "Restart a Universal Link" on the next page.

Link Details Page

The Link Details page shows status information for configured log sources, including timestamp for the last data received, the number of events in the last batch of data, and whether the configuration is active.

To display the Link Details page, from the Link summary page, click the hyperlink in the Name column to display the Link details page for the Link you want to review. The following figure shows the Link Details page for a Universal Link instance.



Restart a Universal Link

	In the Link tools panel, click the Restart icon.

Copy a Link ID

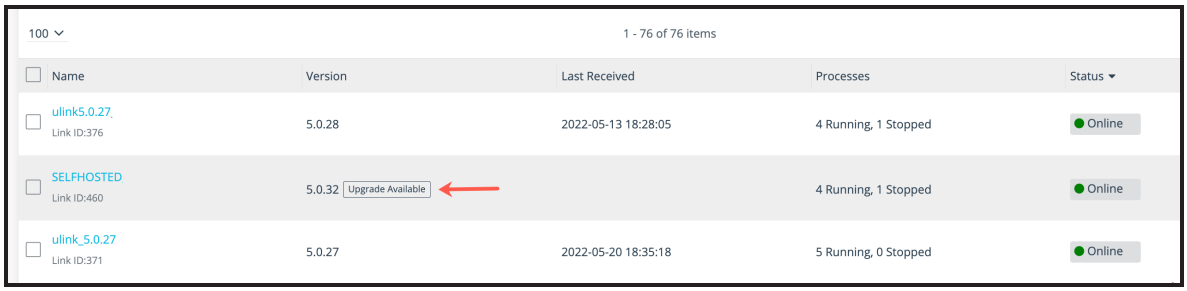
	Hover over the Link ID text on the Link summary or Link details page and click the Copy icon.

Upgrade Link Software

Universal Link 5.0.32 and later can be upgraded from the Security Analytics **Settings** > **Links** page.

> **Note:** Anomali Link for Splunk and earlier versions of Universal Link must be upgraded manually. For details, see the installation guide for the Anomali Link software.

The Link Summary page displays and Upgrade Available notification in the Version column when a new version is available.



To upgrade:

1. Click the Settings icon in the left navigation panel and select **Security Analytics**.
2. Click **Links**.
3. Click **Universal Links**.
4. Click the hyperlink name of Link that shows an upgrade available to display the Link Details page.
5. Click **Upgrade** in the Link tools panel to initiate the upgrade.

6. Confirm you want to upgrade the software.

Create a Link Configuration

Anomali Cloud Link instances are created by Anomali. Please contact Anomali Customer Support to request cloud-to-cloud log ingestion.

Anomali Universal Link and Anomali Link for Splunk autoregister with Security Analytics upon installation, so you typically do not need to create or modify those configurations.

Splunk Link

Anomali Link for Splunk autoregisters with Security Analytics upon installation, so you typically do not need to create or modify the configurations. If necessary, you can create a new Splunk configuration from within Security Analytics.

To create an Anomali Link for Splunk configuration:

1. Click the Settings icon in the left navigation panel and select **Security Analytics**.
2. Click **Links**.
3. Click **Splunk Links** in the left navigation menu.
4. Click **Actions** and select **Create New Link**.

The Splunk Link configuration form is displayed.

5. Complete the configuration as described in the following table.

Setting	Description
Name	Type a name that facilitates Link management. Only ASCII characters are allowed. Maximum 100 characters.
Type	Splunk.
Splunk User Name	User name that has been configured to authenticate to the Splunk instance.
Password	The corresponding password.
Splunk Management URL	The URL for the management port of this Splunk instance. For example: https://<splunk_server_IP>:8089 When the Link is set up on the Splunk deployer, the URL is either https://<splunk_cluster_search_head_IP>:8089 or <https://splunk_cluster_ load_balancer_IP:8089>.
Drilldown Limit	This is the maximum number of rows returned by the drilldown. Default is 100 rows.
Index Filter	Default is: index=main

6. Click **Save**.

Modify a Link Configuration

If necessary, you can modify Link settings.

Universal Link

Universal Link autoregisters with Security Analytics with a proper configuration. You typically do not have to modify link configuration settings, but it is possible to modify.

To modify a Universal Link configuration:

1. Click the Settings icon in the left navigation panel and select **Security Analytics**.
2. Click **Links**.
3. Click **Universal Links** in the left navigation menu and then click the name of the Link you want to modify.
4. Click the Settings icon in the Link tools panel.

The Link configuration editor is displayed.

5. Modify the configuration as described in the following table.

Setting	Description
Name	Type a name that facilitates Link management. Only ASCII characters are allowed. Maximum 100 characters.
Type	Universal Link.
Universal Link Version	Version of Universal Link. This field is auto-populated once registration with Universal Link succeeds.
Link Connection Timeout	The period after which Universal Link is not connected to Anomali Security Analytics. The default timeout period is 5 seconds. Edit this field to set a different timeout period.
Internal Network	One or more IP addresses or IP address ranges in your network that can send data through this Universal Link. Click inside the field and select one or more address ranges in your internal network, or add more IP address ranges in your network.
Advanced Settings	Select **Enable debug logging events** only when instructed by Anomali support.

6. Click **Save**.

Splunk Link

Anomali Link for Splunk autoregisters with Security Analytics with a proper configuration. You typically do not have to modify link configuration settings, but it is possible to modify.

To modify an Anomali Link for Splunk configuration:

1. Click **Links** in the left navigation menu.
2. Locate the Splunk Link configuration you want to edit and click the hyperlink in the Name column.

   The Link configuration editor is displayed.

3. Complete the configuration as described in the following table.

Setting	Description
Name	Type a name that facilitates Link management. Only ASCII characters are allowed. Maximum 100 characters.
Type	Splunk.
Splunk User Name	User name that has been configured to authenticate to the Splunk instance.
Password	The corresponding password.
Splunk Management URL	The URL for the management port of this Splunk instance. For example: https://<splunk_server_IP>:8089 When the Link is set up on the Splunk deployer, the URL is either https://<splunk_cluster_search_head_IP>:8089 or <https://splunk_cluster_ load_balancer_IP:8089>.
Drilldown Limit	This is the maximum number of rows returned by the drilldown. Default is 100 rows.
Index Filter	Default is: index=main

4. Click **Save**.

Regenerate a Universal Link Configuration

Regenerate Now	In the Link tools panel, click the **Regenerate Now**.

Delete a Link Configuration

Select a Link configuration in the leftmost column of the table, click **Actions**, and select **Delete**.

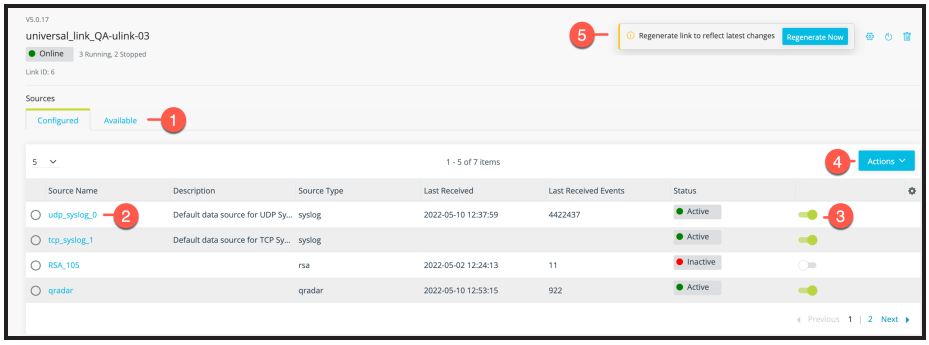
Tip: You can also delete active Universal Link configurations from the Link details page. In the Link tools panel, click the Delete icon ( ).

Manage Log Source Configurations

Note:

- You can add use the Security Analytics user interface to add log sources and manage active/inactive status for on-prem-to-cloud data flows through Universal Link.
- Anomali Customer Support will facilitate the onboarding and management of log sources for cloud-to-cloud data flows.

The following figure shows the tools provided on the Link details page for managing your Universal Link OnPrem log sources.



1	**Configured / Available tabs:** Manage configured log sources or click the **Available** tab to get started with a new log source. See "Add a Log Source Configuration" on the next page.

2	**Edit log source**: Click the hyperlink in the Name column to edit the log source configuration. See "Edit a Log Source Configuration" on page 319.
3	**Activate / Deactivate toggle**: Change active status of the log source. See "Activate a Log Source Configuration" on page 319.
4	**Actions**: Select a log source in the leftmost column of the table, click **Actions**, and select an action: • **Refresh**: Send health status queries and refresh the status indicators. • **Clone**: Create an editable copy of a configuration. See "Clone a Log Source Configuration" on page 320. • **Delete**: Delete an inactive configuration. See "Delete a Log Source Configuration" on page 320.
5	**Regenerate**: For many log source types, after you add a log source, you must regenerate the Link configuration. Click **Regenerate Now** in the Link toolbar. See "Regenerate a Universal Link Configuration" on page 314. Note: This does not apply to "no link" log sources and some Universal Link and Cloud Link types.

Add a Log Source Configuration

The following table summarizes telemetry log sources that have been tested for enterprise deployments. Click the hyperlink in the Log Source column for complete details about adding a log source configuration for the log source type.

Not on the list? Talk to your Anomali representative about any other log sources that you want to use the Anomali platform to analyze.

Log Source	Link Software
1Password	Cloud Link
AWS CloudTrail	Cloud Link
AWS GuardDuty	Cloud Link
AWS Load Balancer	Cloud Link
AWS VPC DNS	Cloud Link
AWS VPC Flow	Cloud Link
Azure Event Hubs	Cloud Link
Azure NSG Flow	Cloud Link
Azure Sentinel	Cloud Link
Carbon Black	Cloud Link
Cloudflare WAF	Cloud Link
Cribl	Cloud Link
CrowdStrike	Cloud Link
Custom	Universal Link
Duo	Cloud Link
Forcepoint	Cloud Link
Fortinet	Universal Link
Generic Syslog	Universal Link
Github Cloud	Cloud Link
Google Cloud Platform (firewall)	Cloud Link
Google Cloud Platform (VPC)	Cloud Link
Google Workspace	Cloud Link

Log Source	Link Software
HA Proxy	Cloud Link
HTTP Upload	Cloud Link
IBM QRadar on Cloud	Cloud Link
IBM QRadar OnPrem	Universal Link
Symantec ICDx	Universal Link
JumpCloud	Cloud Link
Kafka	Universal Link
Linux Server Audit	Cloud Link
Linux Server Auth	Cloud Link
Microsoft Defender	Cloud Link
Microsoft Defender ATP	Cloud Link
Microsoft Office 365	Cloud Link
Mimecast	Cloud Link
NetFlow	Universal Link
Netskope	Cloud Link
NXLog	Cloud Link
Okta	Cloud Link
Palo Alto Networks firewall	Cloud Link
RSA NetWitness	Universal Link
sFlow	Universal Link
Splunk	Splunk Link
Sumo Logic	Cloud Link
Suricata Cloud-to-Cloud	Cloud Link

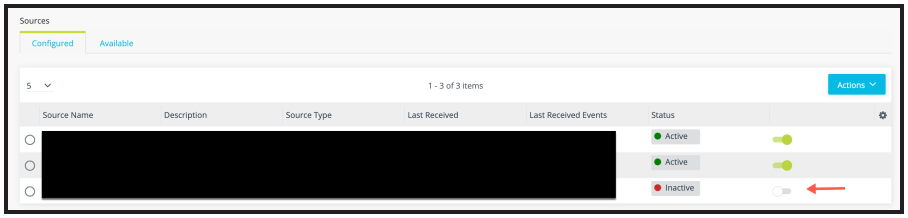
Log Source	Link Software
Suricata (OnPrem-to-Cloud)	Universal Link
Winlogbeat	Universal Link

Activate a Log Source Configuration

By default, newly configured log sources are not active.

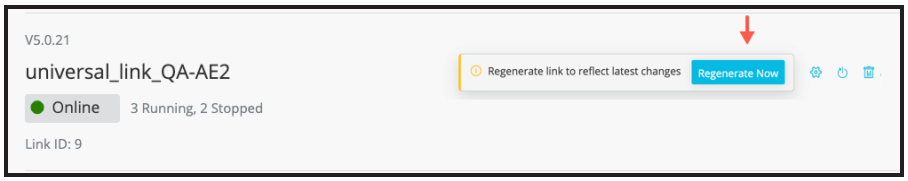
To activate a log source:

1. Click the Settings icon in the left navigation panel and select **Security Analytics**.
2. Click **Links**.
3. Click **Universal Links** in the left navigation menu and then click the name of the Link you want to modify.
4. Locate the log source you want to modify and toggle the activation switch shown in the following figure.



5. A Universal Link configuration must be regenerated before modifications go into effect.

   Click **Regenerate Now** in the Link tools panel.



Edit a Log Source Configuration

You can edit log source configuration settings as needed. The configuration can be edited only when it is inactive.

To edit a log source configuration:

1. Click the Settings icon in the left navigation panel and select **Security Analytics**.
2. Click **Links**.
3. Click **Universal Links** in the left navigation menu and then click the name of the Link you want to modify.
4. Click the Active toggle to deactivate the log source, if necessary.
5. Under Sources, on the Configured tab, click the name of the hyperlink in the Source Name column of the configuration you want to modify.
6. Make your changes.
7. Save the configuration.

Clone a Log Source Configuration

You can create a clone (an editable copy) of a log source configuration.

To clone a log source configuration:

1. Click the Settings icon in the left navigation panel and select **Security Analytics**.
2. Click **Links**.
3. Click **Universal Links** in the left navigation menu and then click the name of the Link you want to modify.
4. Locate the log source configuration you want to clone and click the selection option in the leftmost column of the table.
5. Click **Actions** and select **Clone**.
6. Edit the copy and give it an appropriate configuration name.
7. Save the configuration.

Delete a Log Source Configuration

You can delete a log source configuration that is no longer active and in use.

To delete a log source configuration:

1. Click the Settings icon in the left navigation panel and select **Security Analytics**.
2. Click **Links**.
3. Click **Universal Links** in the left navigation menu and then click the name of the Link you want to modify.
4. Locate the log source configuration you want to delete and click the selection option in the leftmost column of the table.
5. Click the Active toggle to deactivate the log source, if necessary.
6. Click **Actions** and select **Delete**.

Managing Asset Data Imports

You use the **Settings** > **Assets** page to import asset data or to create manual entries.

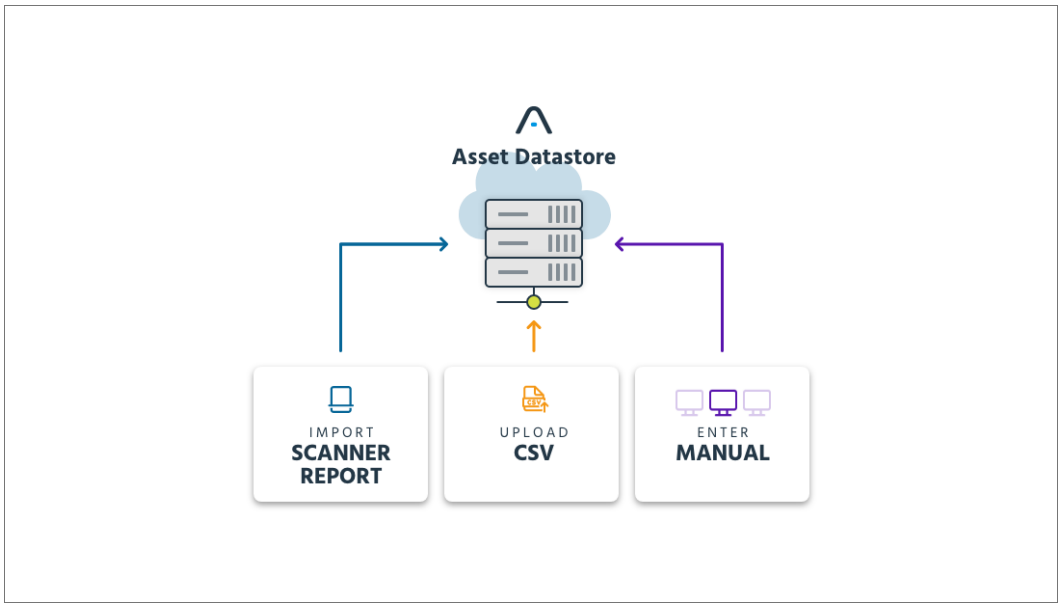
> **Note:** When you get started with your Security Analytics deployment, import asset data before you ingest event log data. The asset data is used during correlation to enrich the results. Correlation occurs only during log ingestion.

About Asset Data Sources

Asset data encompasses details that your IT organization maintains about computer systems on your network, including hostname, IP address, MAC address, department, criticality, location, and operating system.

Asset data is used to enrich search results with asset-related fields. The enriched results make it easier for you to set up operations to monitor and report on impacted assets.

You can import asset data from Qualys scanners, Rapid7 scanners, Tenable scanners, as well as CSV files you upload or import from AWS SQS or S3 bucket locations. You can also create asset records manually.



You may have imports from multiple instances of scanners or multiple types of scanners. IP address is the primary key for the asset database and is used to de-duplicate entries. If scanner reports include the same assets (for example, two entries with the same IP address), the latest entry is applied. In other words, the earlier record for the asset is overwritten. If you do not want this behavior, reconfigure the scanners to report on mutually exclusive sets of assets.

> **Note:** After you have added asset data via scanner report, CSV file, or manual entry, the update is processed to be included in Activity search. It takes up to ten minutes for the data to be available in Activity search.

Managing Qualys Scanner Imports

Anomali Security Analytics supports asset report imports from Qualys Cloud.

About Qualys Scanner Imports

When you configure integration with the scanner from Security Analytics, you must specify scanner connection information, including the scanner fully-qualified domain name (FQDN) or IP address and authentication and authorization credentials.

Create a New Scanner Configuration

To import assets from a Qualys scanner:

1. Click the Settings icon in the left navigation panel and select **Security Analytics**.
2. Click **Assets**.
3. Click the **Scanner** tab.
4. Click **Create New Scanner**.
5. Complete the configuration as described in the following table.

Setting	Description
Scanner	Select **Qualys**.
Name	A meaningful configuration name.
Host	Specify the Qualys API server URL, without the protocol (without https://). For example, if the UI platform URL is `https://qualysguard.qualys.com`, specify the API URL as `qualysapi.qualys.com`. Refer to the following resources from Qualys to look up the API Server URL that applies to your Qualys instance: ■ Qualys topic, "Identify your Qualys platform" ■ Qualys topic, "URL to Qualys API server" **Important**: In Security Analytics, specify the variation of the URL that includes `api`.
Username	User name for connecting to the scanner service.
Password	Password associated with the scanner service.

6. Click **Next**.
7. Specify the schedule and the type of search as described in the following table.

Setting	Description
Sync Data	Specify the schedule for the sync job: ■ Interval: Select every **1 day**, **2 days**, **7 days**, **14 days**, or **28 days**; or select a day of the week to set up weekly scans. ■ Start time: Type the hour (0-23) and minute (0-59). **Note**: The time you specify for asset scanner sync jobs is UTC time with no time zone offset. For example, if you specify the start time for the sync job to be 12:00, it runs at 12:00 UTC, which is 05:00 in Los Angeles and 13:00 in Belfast.
Scan events for the last	Specify the time range for returning asset information from the scans in the following format: *n* [Days | Hours | Minutes]
Search Type	■ **IP/IP range**: Specify IP addresses and IP ranges (separated by a comma). For example, 192.0.2.5, 192.168.1.1-192.168.1.10, 203.0.113.47 IP addresses in the range must have the same first octet. For example, 172.x.x.x - 172.x.x.x If multiple IP ranges are specified, they should not have overlapping IP addresses. ■ **Asset groups**: Specify asset groups created on the scanner system. When new groups are created on the scanner service, click ⟲ to get an updated list of groups, and add them to Security Analytics as needed.

8. Click **Save**.

Notes:

- When the scanner configuration is initially activated, Anomali Security Analytics queries Qualys to scan for the period specified by the **Scan events for the last** setting. Subsequently, at the time specified by the **Each Sync** data interval, Security Analytics queries Qualys for the delta (the difference) resulting from changes during the interval period.
- If you change the **Scan events for the last** setting, or if you toggle activation off and on again, Security Analytics again queries Qualys for the full period specified by the **Scan events for the last** setting.

Toggle Activation for a Scanner Configuration

	In the Active column, click the checkbox to make the scanner configuration active or inactive.

Modify a Scanner Configuration

	In the Actions column, click the Edit icon to modify a scanner configuration.

Clone a Scanner Configuration

	In the Actions column, click the Clone icon to create an editable copy of a configuration.

Delete a Scanner Configuration

	In the Actions column, click the Delete icon to delete a scanner configuration.

Preview a Scanner Configuration

	In the Actions column, click the Preview icon to view the scanner configuration details and to see a detailed history of updates from the scanner. The history is a chronology of successful jobs and jobs that may have terminated due to an error.

Managing Rapid7 Scanner Imports

Anomali Security Analytics supports asset report imports from Rapid7 InsightVM Platform.

About Rapid7 Scanner Imports

When you configure an integration with the scanner from Security Analytics, you must specify scanner connection information, including the Rapid7 region and the API key for your Rapid7 InsightVM Platform account.

The Security Analytics queries to Rapid7 return the following fields which populate Security Analytics asset datastore records:

- IP address
- MAC address
- Hostname
- Operating system
- Vulnerabilties (CVEs)
- Asset date

Create a New Scanner Configuration

To import assets from a Rapid7 scanner:

1. Click the Settings icon in the left navigation panel and select **Security Analytics**.
2. Click **Assets**.
3. Click the **Scanner** tab.
4. Click **Create New Scanner**.
5. Complete the configuration as described in the following table.

Setting	Description
Scanner	Select **Rapid7 InsightVM Platform**.
Name	A meaningful configuration name.

Setting	Description
Region	Select your Rapid7 region. Refer to the Rapid7 topic, "Check your data region," for a pointer on how to look up the region provisioned for your organization.
API Key	Paste the API key that has authorization to the desired assets. It does not matter if the API key is a platform, organization, or user API key. Refer to the Rapid7 topic, "Managing Platform API Keys," for details on how to look up the API key.

6. Click **Next**.
7. Specify the schedule and the type of search as described in the following table.

Setting	Description
Sync Data	Specify the schedule for the sync job: ■ Interval: Select every **1 day**, **2 days**, **7 days**, **14 days**, or **28 days**. ■ Start time: Type the hour (0-23) and minute (0-59). **Note**: The time you specify for asset scanner sync jobs is UTC time with no time zone offset. For example, if you specify the start time for the sync job to be 12:00, it runs at 12:00 UTC, which is 05:00 in Los Angeles and 13:00 in Belfast.
Scan events for the last	Specify the time range for returning asset information from the scans in the following format: *n* days

8. Click **Save**.

Notes:

- When the scanner configuration is initially activated, Anomali Security Analytics queries Rapid7 to scan for the period specified by the **Scan events for the last** setting. Subsequently, at the time specified by the **Each Sync** data interval, Security Analytics queries Rapid7 for the delta (the difference) resulting from changes during the interval period.
- If you change the **Scan events for the last** setting, or if you toggle activation off and on again, Security Analytics again queries Rapid7 for the full period specified by the **Scan events for the last** setting.

Toggle Activation for a Scanner Configuration

	In the Active column, click the checkbox to make the scanner configuration active or inactive.

Modify a Scanner Configuration

	In the Actions column, click the Edit icon to modify a scanner configuration. **Note**: You are prompted to enter the API key to save changes to the scanner configuration.

Clone a Scanner Configuration

	In the Actions column, click the Clone icon to create an editable copy of a configuration. **Note**: You are prompted to enter the API key to save a cloned copy of the scanner configuration.

Delete a Scanner Configuration

	In the Actions column, click the Delete icon to delete a scanner configuration.

Preview a Scanner Configuration

	In the Actions column, click the Preview icon to view the scanner configuration details and to see a detailed history of updates from the scanner. The history is a chronology of successful jobs and jobs that may have terminated due to an error.

Managing Tenable Scanner Imports

Anomali Security Analytics has tested asset report imports from the following Tenable scanners:

- Tenable.io
- Tenable.sc 5.9

About Tenable.io API Requests

Security Analytics uses the pytenable python library and uses the following methods to fetch the assets and the vulnerability information:

- `tio.exports.assets(updated_at=ts)`
- `tio.exports.vulns(since=ts)`

Security Analytics sends requests to the following Tenable endpoints to start the download, check the status if the request is ready, and to download in chunks:

- https://cloud.tenable.com/assets/export
- https://cloud.tenable.com/assets/export/{export_uuid}/status
- https://cloud.tenable.com/assets/export/{export_uuid}/chunks/{chunk_id}
- https://cloud.tenable.com/vulns/export
- https://cloud.tenable.com/vulns/export/{export_uuid}/status
- https://cloud.tenable.com/vulns/export/{export_uuid}/chunks/{chunk_id}

In addition, if you enable the option to share new asset information with Tenable.io, Security Analytics sends requests to the following endpoint:

- https://cloud.tenable.com/import/assets

In Security Analytics, when you configure the connection to Tenable.io, the Access Key you specify must be associated with a Tenable Administrator account. Per Tenable documentation, Administrator permissions are required to manage asset data exports and vulnerability data exports.

Create a Tenable.io Configuration

When you configure integration with the scanner from Security Analytics, you must specify scanner connection information, including authentication and authorization credentials.

To configure import from a Tenable.io scanner:

1. Click the Settings icon in the left navigation panel and select **Security Analytics**.
2. Click **Assets**.
3. Click the **Scanner** tab.
4. Click **Create New Scanner**.
5. Complete the configuration as described in the following table.

Setting	Description
Scanner	Select **Tenable.io**.
Name	A meaningful configuration name.
Access Key	Specify the Tenable instance access key. The Access Key you specify must be associated with a Tenable Administrator account. Per Tenable documentation, Administrator permissions are required to manage asset data exports and vulnerability data exports.
Secret Key	Specify the Tenable instance secret key.

Setting	Description
Share new asset information with Tenable IO	Select this option to enable Security Analytics to be a source of asset data to Tenable IO. If selected, Security Analytics sends Tenable IO asset records that are from sources other than Tenable IO.

6. Click **Next**.
7. Specify the schedule as described in the following table.

Setting	Description
Sync Data	Specify the schedule for the sync job to run: ■ Interval: Select every **1 day**, **2 days**, **7 days**, **14 days**, or **28 days**. ■ Start time: Type the hour (0-23) and minute (0-59). ■ **Notes**: ○ Security Analytics initiates API requests based on the schedule you set up here. It does not depend on the time scans are completed on the Tenable server. ○ The time you specify for asset scanner sync jobs is UTC time with no time zone offset. For example, if you specify the start time for the sync job to be 12:00, it runs at 12:00 UTC, which is 05:00 in Los Angeles and 13:00 in Belfast.
Scan events for the last	Specify the time range for returning asset information from the scans in the following format: *n* [Days | Hours | Minutes]

8. Click **Save**.

Notes:

- When the scanner configuration is initially activated, Anomali Security Analytics queries Tenable.io to scan for the period specified by the **Scan events for the last** setting. Subsequently, at the time specified by the **Each Sync** data interval, Security Analytics queries Tenable.io for the delta (the difference) resulting from changes during the interval period.
- If you change the **Scan events for the last** setting, or if you toggle activation off and on again, Security Analytics again queries Tenable.io for the full period specified by the **Scan events for the last** setting.

Create a Tenable.sc Configuration

When you configure integration with the scanner from Security Analytics, you must specify scanner connection information, including authentication and authorization credentials. For Tenable.sc, you must specify the fully-qualified domain name (FQDN) or IP address for the scanner.

To configure import from a Tenable.sc scanner:

1. Click the Settings icon in the left navigation panel and select **Security Analytics**.
2. Click **Assets**.
3. Click the **Scanner** tab.
4. Click **Create New Scanner**.
5. Complete the configuration as described in the following table.

Setting	Description
Scanner	Select **Tenable.sc**.
Name	A meaningful configuration name.
Host	Host name or FQDN of the scanner service.

Setting	Description
Access Key	Specify the Tenable instance access key.
Secret Key	Specify the Tenable instance secret key.

6. Click **Next**.
7. Specify the schedule and the type of search as described in the following table.

Setting	Description
Sync Data	Specify the schedule for the sync job to run: ■ Interval: Select every **1 day**, **2 days**, **7 days**, **14 days**, or **28 days**. ■ Start time: Type the hour (0-23) and minute (0-59). **Note**: The time you specify for asset scanner sync jobs is UTC time with no time zone offset. For example, if you specify the start time for the sync job to be 12:00, it runs at 12:00 UTC, which is 05:00 in Los Angeles and 13:00 in Belfast.
Scan events for the last	Specify the time range for returning asset information from the scans in the following format: *n* [Days | Hours | Minutes]

Setting	Description
Search Type	▪ Click in the **Specify Queries** search field to get a list of available queries defined in Tenable.sc. Select the queries you want to add. The selected queries are displayed in the field below. ▪ When new queries are created in the scanner service, click the Refresh icon ( ) to get an updated list, and then add them to Security Analytics as needed. **Note:** The Severity = Minor setting from tenable.sc is mapped to Criticality = Low in Security Analytics.

8. Click **Save**.

> **Note:** In contrast to the Tenable.io integration, which can perform delta queries, the Tenable.sc integration requires Security Analytics to query Tenable.sc for the full interval specified by the Scan events for the last setting.

Toggle Activation for a Scanner Configuration

	In the Active column, click the checkbox to make the scanner configuration active or inactive.

Modify a Scanner Configuration

	In the Actions column, click the Edit icon to modify a scanner configuration.

Clone a Scanner Configuration

	In the Actions column, click the Clone icon to create an editable copy of a configuration.

Delete a Scanner Configuration

	In the Actions column, click the Delete icon to delete a scanner configuration.

Preview a Scanner Configuration

	In the Actions column, click the Preview icon to view the scanner configuration details and to see a detailed history of updates from the scanner. The history is a chronology of successful jobs and jobs that may have terminated due to an error.

Managing AWS Asset Data Imports

Anomali Security Analytics supports scheduled asset data imports from AWS SQS or S3 locations.

About AWS Assert Data Imports

When you configure scheduled imports from AWS, you must specify the AWS SQS URL or S3 bucket details, as well as the AWS access key and secret key provisioned for this integration.

You can ingest the following file types:

- JSON
- CSV
- tar.gz (containing JSON or CSV files)

When you set up your asset import, you set up mapping from your source fields to the following Security Analytics asset fields:

- time
- ip (required)
- hostname
- os
- criticality
- count
- vulnerabilities
- scanner

- source
- mac
- netbios
- fqdns
- owner
- tags (you can map multiple source fields to the Security Analytics **tags** field)

Collect Credentials to Use for the Connection from Anomali Security Analytics

Your AWS administrator (with admin role permissions) must create a dedicated AWS Identity and Access Management (IAM) account for the integration with Security Analytics. Security Analytics will use this account to connect to your resources (AWS S3 bucket or AWS SQS queue) to retrieve the asset data.

Typically, an organization grants resource access permissions through AWS administration groups as follows:

- Sets up an administration group for the specific purpose of supporting the integration.
- Associates a policy with the administration group.
- Creates an IAM account and associates the account with the administration group.

The following example shows an IAM resource access policy configured to grant the permissions required for this integration.

```
{
        "Version": "2012-10-17",
        "Statement": [
                {
                        "Sid": "resourcePermission",
                        "Effect": "Allow",
                        "Action": [
                                "s3:GetObject",
                                "s3:ListBucket",
                                "s3:GetBucketLocation"
                        ],
                        "Resource": [
                                "arn:aws:s3:::<bucket-name>/*",
                                "arn:aws:s3:::<bucket-name>"
                        ]
```

```
                },
                {
                        "Sid": "VisualEditor0",
                        "Effect": "Allow",
                        "Action": [
                                "sqs:ChangeMessageVisibility",
                                "sqs:DeleteMessage",
                                "sqs:GetQueueAttributes",
                                "sqs:ReceiveMessage",
                                "sqs:SendMessage"
                        ],
                        "Resource": "<SQS-queue-ARN>"
                }
        ]
}
```

Specify your resource IDs in place of the placeholders <bucket-name> and <SQS-queue-ARN> that are used in the example.

For details about IAM policies, refer to the AWS topic, "Creating IAM policies."

The following table explains the required IAM resource access permissions.

AWS S3	s3:GetObject Grants access to retrieve objects from S3 buckets. S3 files are related to the SQS event being processed.
	s3:ListBucket Grants access to list the content of an S3 bucket. S3 works through a polling mechanism by listing the bucket content every time and processing newer files.
	s3:GetBucketLocation Grants access to retrieve a bucket Region location, used to connect later by specifying the proper region.

AWS SQS QUeue	s3:GetObject Grants access to retrieve objects from S3 buckets. S3 files are related to the SQS event being processed.
	sqs:DeleteMessage Grants access to remove a message from the queue. Given the distributed nature of SQS consumers, consumers must acknowledge receipt by deleting the message.
	sqs:ChangeMessageVisibility Grants access to modify the SQS message visibility timeout–a time window until the message is made available in the queue again if a consumer did not acknowledge receipt.
	sqs:GetQueueAttributes Grants access to read the SQS queue attributes. This is used to validate access for the given key pair.
	sqs:ReceiveMessage Grants access to reading messages from the SQS queue.

Once the AWS IAM account is created, create and retrieve an Access Key needed to connect to the resources as described in the AWS topic, "Managing access keys for IAM users > Managing access keys (console)."

Copy the Access key ID and Secret access key values that will be needed when you create the Security Analytics asset scanner configuration.

Create a New Scanner Configuration

To import assets from AWS:

1. Click the Settings icon in the left navigation panel and select **Security Analytics**.
2. Click **Assets**.
3. Click the **Scanner** tab.
4. Click **Create New Scanner**.
5. Select **AWS**.

6. Complete the configuration as described in the following table.

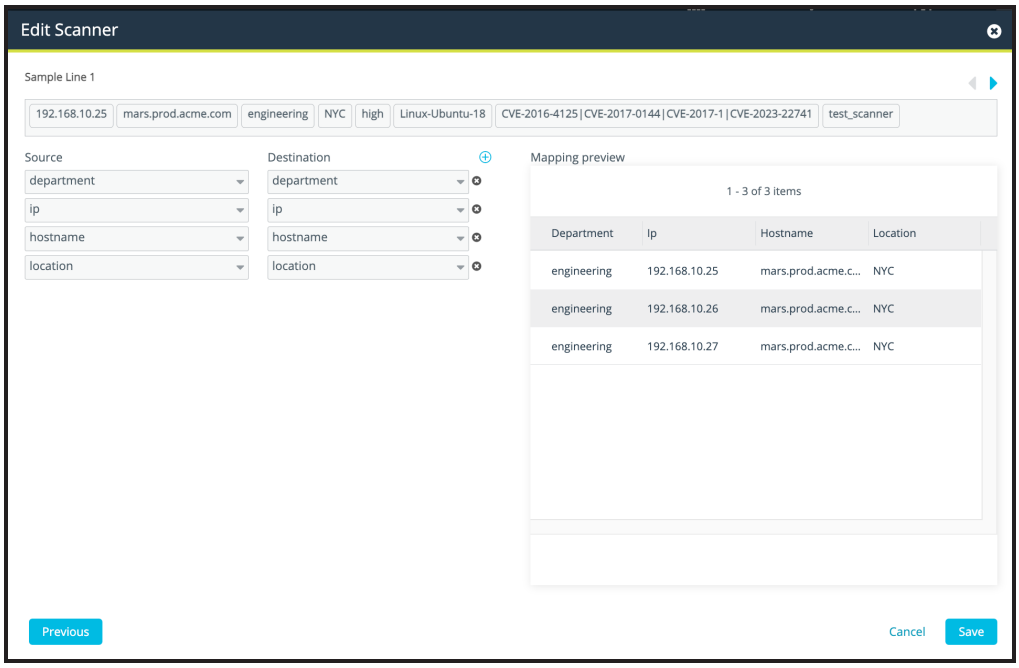
Setting	Description
Name	A meaningful configuration name.
Import Type: SQS	**SQS URL**: Specify the SQS Queue URL from which Security Analytics will ingest asset data.
Import Type: S3	**S3 Bucket ARNs**: Specify the s3 bucket location in ARN format: `arn:aws:s3:::bucket_name/key_name`
	S3 Bucket Prefix: Specify a comma-separated list of object prefixes. A prefix must include the trailing slash character. For example: `user_uploaded_assets/,test_prefixes/`
Access Key	Specify the account provisioned for this integration.
Secret Key	Specify the secret key corresponding with the access key.

7. Click **Next**.

8. Specify the schedule and the type of search as described in the following table.

Setting	Description
Sync Data	Specify the schedule for the sync job: ■ Interval: Select every **1 day**, **2 days**, **7 days**, **14 days**, or **28 days**. ■ Start time: Type the hour (0-23) and minute (0-59). **Note**: The time you specify for asset scanner sync jobs is UTC time with no time zone offset. For example, if you specify the start time for the sync job to be 12:00, it runs at 12:00 UTC, which is 05:00 in Los Angeles and 13:00 in Belfast.
Scan events for the last	Specify the time range for returning asset information from the AWS location in the following format: *n* days
Sample Content	Paste a sample from the source data that includes the CSV lines or JSON elements that are to be parsed by Security Analytics upon import.
Parser Type	Select the data format used in the source data: CSV or JSON.
Delimiter	For CSV data, select the column delimiter used in the source data: pipe, comma, semi-colon, or space.
Sample contains header	For CSV data, select this option if the first row of the sample is a header row.

9. Click **Next** to display the mapping page.



The top section shows the raw data from your log source. Use the Source and Destination drop down menus on the left to map the data to Security Analytics asset fields. The Mapping Preview on the right shows the resulting Security Analytics asset table.

Notes:

- You must include the **ip** field in the mapping. IP address is the primary key used to uniquely identify an asset in the Security Analytics asset data store.
- You can map multiple source fields to the Security Analytics **tags** field.

10. Click **Save**.

Notes:

S3	When the import job runs at the scheduled time, Security Analytics imports files having a modified_ timestamp value that falls within the number of days specified by the **Scan events for the last** setting. At the next scheduled time, Security Analytics imports files having a modified_timestamp value that falls within its collection window, so only files modified or created since the previous run are imported.
SQS	When the import job runs at the scheduled time, Security Analytics processes the messages in the SQS queue at that time. The messages are removed from the SQS queue once they are processed, so they are not available to be processed in the next run.

Toggle Activation for a Scanner Configuration

	In the Active column, click the checkbox to make the scanner configuration active or inactive.

Modify a Scanner Configuration

	In the Actions column, click the Edit icon to modify a scanner configuration.

Clone a Scanner Configuration

	In the Actions column, click the Clone icon to create an editable copy of a configuration.

Delete a Scanner Configuration

	In the Actions column, click the Delete icon to delete a scanner configuration.

Preview a Scanner Configuration

	In the Actions column, click the Preview icon to view the scanner configuration details and to see a detailed history of updates from the scanner. The history is a chronology of successful jobs and jobs that may have terminated due to an error.

Managing Asset CSV File Imports

You can import comma-separated value (CSV) files that contain asset data.

About CSV File Imports

Use the CSV file template files that are provided to ensure the asset data model can be imported and parsed appropriately. The asset data maintained for your IT organization may be suited to one or more of the template types.

IP Address Mapping

The IP Address Mapping option requires you to fill out a single template (template_ip_to_hostname.csv). This option is recommended when you have a list of IP addresses mapped to hostnames or IP address ranges (in CIDR format) mapped to group names.

The uploaded file must:

- Have the `.csv` file extension.

  If you are saving the file using MS Excel, make sure you select a Save option that saves the contents to a comma-separated or comma-delimited file.

- Contain the following headers, in lowercase: **`ip`**, **`hostname`**, `department`, `location`, **`criticality`**

  Fields shown in bold must contain values. All others can be blank. The headers must be in lowercase. Values for these fields can be in any case.

- Separate fields with a comma.

The following example shows the format of the CSV list in template_ip_to_hostname.csv:

```
ip,hostname,department,location,criticality,os,vulnerabilities,sca
nner
```

The following example shows example values for template_ip_to_hostname.csv:

```
192.168.10.25,mars.prod.acme.com,engineering,NYC,high, Linux-Ubuntu-18, CVE-2018-10561|CVE-2020-0822, test_scanner
192.168.50.0/24,sales servers,Sales,Washington D.C.,critical, Linux-Ubuntu-18, CVE-2014-2483, test_scanner
```

MAC address mapping

The MAC address mapping option requires you to fill out two CSV templates (template_mac_to_hostname.csv and template_ip_to_mac.csv). This option is useful in environments where MAC address to hostname information does not change on a regular basis, however, IP address to MAC address is dynamic and short lived. For example, if DHCP is used to allocate IP addresses to assets in your network, MAC address to hostname information will not change as frequently as the IP address to MAC address information.

Once uploaded, the two files are merged to establish an IP address to hostname relationship (since mac is a common field in both files).

The uploaded file must:

- Have the `.csv` file extension

  If you are saving the file using MS Excel, make sure you select a Save option that saves the contents in a comma-separated or comma-delimited file.

- Contain the following headers, in lowercase:

  MAC address to hostname file: **`mac`**, **`hostname`**, `department`, `location`, **`criticality`**

  IP address to MAC address file: **`ip`**, **`mac`**

  Fields shown in bold must contain values. All others can be blank. The headers must be in lowercase. Values for these fields can be in any case.

- Separate fields with a comma.

The following example shows the format of the CSV list in the template_mac_to_hostname.csv template:

```
mac,hostname,department,location,criticality
```

The following example shows example values for this template:

```
38:c9:86:4a:61:bc,rsmith.local,IT,SF,medium
c8:69:cd:af:25:ca,jdole.local,engineer,SF,low
```

The following example shows the format of the CSV list in the template_ip_to_hostname.csv template:

Format: `ip,mac`

The following example shows example values for this template:

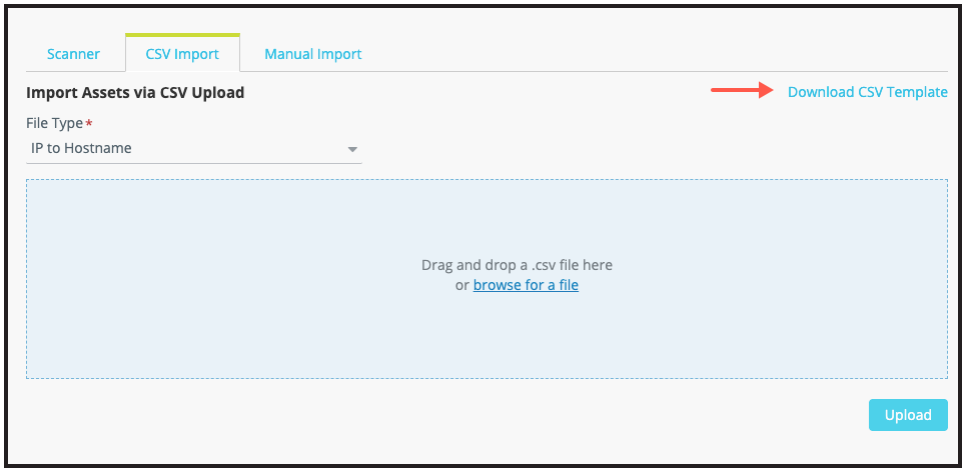
```
192.168.20.5,38:c9:86:4a:61:bc
192.168.20.110,c8:69:cd:af:25:ca
```

Download CSV File Templates

Download the CSV template files and fill them out or use them as a reference to ensure your own CSV files conform with the expected format.

To download the CSV templates:

1. Click the Settings icon in the left navigation panel and select **Security Analytics**.
2. Click **Assets**.
3. Click the **CSV Imports** tab.
4. Click **Download CSV Template** link.



5. Click the links to download the single IP Address Mapping template and/or the set of two MAC address mapping templates.
6. Click **OK** to dismiss the dialog box.

Upload a CSV File

Upload the completed CSV files to enable enrichment with asset details. A new upload overwrites records for an asset that has the same IP address.

> **Note:**
>
> - The first time you upload the MAC address mapping templates, you must upload both files together: mac_to_hostname.csv and ip_to_mac.csv.
> - Subsequent uploads can include only the file that has changed.

To upload a CSV file:

1. Click the Settings icon in the left navigation panel and select **Security Analytics**.
2. Click **Assets**.
3. Click the **CSV Imports** tab.
4. Select a template file type from the drop-down list.
5. Drag and drop your CSV file to the highlighted area or click the browse link to locate and select your file.
6. Click **Upload**.

Adding Manual Entries

You can add manual asset data entries if necessary.

To add a manual entry:

1. Click the Settings icon in the left navigation panel and select **Security Analytics**.
2. Click **Assets**.
3. Click the **Manual Import** tab.
4. Select an asset model type from the File Type list.

> **Note:** You must complete the MAC description settings for an asset to add it to the database. If updates are required after you have created the asset record, you can use the IP to MAC mapping settings to update the record.

File Types	
Asset mapping	To add IP address to hostname mapping
IP to MAC mapping	To add IP address to MAC address mapping
MAC description	To add MAC address to hostname mapping

5. Complete the configuration as described in the following table.

File Types	Setting	Description
Asset mapping	IP Address	IP address of the asset. Specify an IP address range in CIDR format to specify all assets in the range.
	Hostname	Hostname of the asset.
	Department	(Optional) Department to which the asset belongs.
	Criticality	Level of criticality assigned to the asset. You can select from Critical, High, Medium, and Low.
	Location	(Optional) Geographic location of the asset.
	OS	IP address of the asset.

File Types	Setting	Description
MAC description	MAC Address	MAC address of the asset.
	Hostname	Hostname of the asset.
	Department	(Optional) Department to which the asset belongs
	Criticality	Level of criticality assigned to the asset. You can select from Critical, High, Medium, and Low.
	Location	(Optional) Geographic location of the asset.
	OS	(Optional) Operating system of the asset.
IP to MAC	IP	IP address of the asset. Specify an IP address range in CIDR format to specify all assets in the range.
	MAC Address	MAC address of the asset.

6. Click **Save**.

Managing Anomali Security Analytics Users

You manage Security Analytics users through ThreatStream.

The following ThreatStream permissions apply to Security Analytics.

Permission	Description
Can use Match	Enables users to access Security Analytics through the link in the ThreatStream top navigation bar. Users that do not have this permission are prevented from accessing the Security Analytics user interface. Read Only users can be given the **Can use Match** permission, thus enabling Read Only users to access the Security Analytics user interface.

Permission	Description
Org Admin	The Org Admin permission in ThreatStream also gives users administrator privileges in Security Analytics. You must have the Org Admin permission to view the Security Analytics Settings menu, to view the Data Usage dashboard, and to manage the saved search configurations of other users.

To manage user permissions:

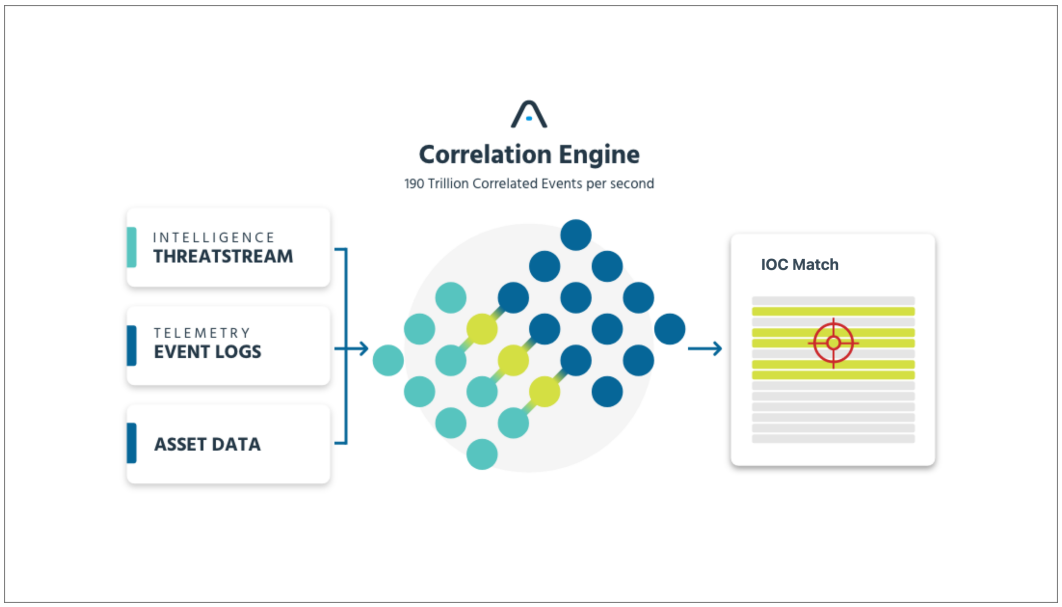
1. Click the Settings icon in the left navigation panel and select **Security Analytics**.
2. Click **Users**.
3. Click the **Manage Users** button to navigate to the ThreatStream User Admin page.
4. Follow the instructions in the ThreatStream online help to manage user permissions.

Modifying IOC Correlation Engine Settings

You can use the **Settings** > **Correlation** page to modify IOC Correlation Engine settings.

About the IOC Correlation Engine

The IOC correlation engine matches indicators defined in ThreatStream intelligence feeds with event logs ingested from Links. The resulting IOC Match table combines the intelligence fields and event fields. If you have imported asset data, the IOC Match table is enriched with asset data associated with logged IP addresses. Correlation and asset enrichment is performed upon log ingestion. Correlated matches are usually available on Activity search pages within minutes.



Indicator values and event log field values must be identical to be considered a match. For example, a Domain indicator having the value `f0563362.xsph.ru` matches any event log field having the value `f0563362.xsph.ru` but not an event log field having the value `a0558863.xsph.ru`. Reporting partial matches would result in too many imprecise records for analysts to examine. Instead, it is customary for a threat intelligence platform to maintain separate precise entries for indicators. In this example, ThreatStream maintains a separate entry for `a0558863.xsph.ru`.

The following table provides examples of correlation matches.

Indicator Value Type	Event Field Value Type	Notes and Examples
Email	Email	Must be an exact match. For example, an APT email indicator with the value `vrickson@mail.com` matches any event log field with the value `vrickson@mail.com`.
Hash	Hash	Must be an exact match. For example, an APT file hash indicator with the value `2f4b376d5f0a6a6e7540c36645bc600c949f4875` matches any event log field with the value `2f4b376d5f0a6a6e7540c36645bc600c949f4875` but not patterns or substrings of the full hash string.

Indicator Value Type	Event Field Value Type	Notes and Examples
IP	IP	Must be an exact match. For example, a Malware C&C IP indicator with the value `104.247.81.50` matches any event log field with the value `104.247.81.50`. Partial matches and pattern matches are not included in the correlated results.
URL	URL	Must be an exact match. For example, a Malware URL indicator with the value `http://121.40.242.232/images/logo.png` matches any event log field with the value `http://121.40.242.232/images/logo.png`. Partial matches are not included in correlated results. For example, an event log field with the value `http://121.40.242.232` would not be included in the correlated results.
Domain	Domain	Must be an exact match. However, Security Analytics parses event log destination URLs to extract domain values. For example, Security Analytics extracts the domain `uyhmgnbvue5j5dbw.onion` from `http://uyhmgnbvue5j5dbw.onion/kpanel/connect.php`. Security Analytics attempts to correlate domain indicators and the extracted domain.

In ThreatStream, indicators have value types Domain, Email, Hash, IP, URL, and String. Security Analytics does not support correlation with indicators having String value types. See "ThreatStream Indicator Types" on page 1028 for a comprehensive list of indicator types (iTypes) available to IOC Match correlation.

Note:

- The daily correlation limit per organization is 3 million IOC Match correlations.
- A single event log can generate multiple correlations (if the event log matches multiple indicators or if you have multiple threat intelligence feeds that report the same indicator).

- When the limit is reached, event log ingestion continues, correlation continues, but the correlation results are not indexed and cannot be searched from the UI for the period that day after the limit was reached.
- You can review event logs for this period in the Forensics & Retrospective Search index, and these logs will show associated ThreatStream IOCs (if any).

Modify IOC Correlation Settings

You can use the settings page to change IOC correlation engine settings.

Note:

- IOC correlation settings do not affect correlation for event logs for *outbound* traffic.
- The IOC correlation settings apply to *inbound* traffic. The default settings exclude event logs having the actions Block, Blocked, Deny, Denied, Drop, Dropped, Reject, and Rejected.
- If you change settings, note that the configuration changes do not change matches that have already been indexed. New settings are effective immediately upon saving the configuration and apply to logs ingested after the setting was changed. In searches for periods before the setting was changed, you will still observe matches for actions that were not excluded when those event logs were ingested.

To change IOC correlation settings:

1. Click the Settings icon in the left navigation panel and select **Security Analytics**.
2. Click **Correlation**.
3. Click the Edit icon ( ) next to **Actions to exclude**.
4. Use the selector controls to move items to and from the exclude list.
5. Click **Save** when you are done.

Chapter 7: User and Role Management

For documentation on the User & Role Management feature, refer to User and Role Management on the Anomali Platform.

Chapter 8: Audit Logging (Limited Availability)

Analysts routinely use Security Analytics to manage their alerts, deploy saved searches, generate reports, or export their search results, generating a large volume of user activity logs.

To reliably track these actions and uncover unexpected changes, as an administrator, you can analyze the activity of users in your organization through audit logs and gain crucial insight into the history of different user actions, ensuring transparency, traceability, compliance, reporting, and accountability for every action initiated by API clients, users, or automated processes.

By capturing information about applications, users, actions, event timestamps, and request specifics such as search queries, audit logging in Anomali ensures your organization operates securely.

Auditing Scope

As an administrator, audit logs help you examine user activity that is logged across the following Security Analytics features:

- Alerts
- Saved searches
- Forensic searches
- Reports
- Exports
- Lookup tables
- Exclude lists
- Dashboards

Additionally, user login and logout activity is logged as well.

Auditable Fields

> **Note**: Depending on the type of log entry, some fields may or may not be populated.

User or API client actions such as create, update, and delete are recorded for the following fields:

`event_time`

Time when the audit log was recorded, in UNIX timestamp milliseconds (in UTC).

`app`

Indicates the application within the platform. Possible values include `api`, `alert`, and `search`.

Application	Description

api	Captures information about API calls that a user makes, including but not limited to:
	• user that made the API call
	• HTTP method (GET, POST, and so on)
	• URI of the request
	• Search Job ID of the search, and more.
	Audit your API call
	Here's a typical search query to audit your API calls:
	`audit | where app = "api"`
	How do I check if my API call failed?
	The following query should help you check what about your API call failed:
	`audit | where app = "api" and status_code = 400`
	This query helps you check which API calls failed and returned the 400 status code. For example,you can use the `request_uri`, `search_query`, and `response_digest` fields to analyze the error.
	`{"message": "line 1:26 missing ')' at '<EOF>'"}`
	In the example `response_digest` JSON object above, the search query is wrong since it is missing a `')'`.

Application	Description

alert	Captures all the details about alerts, including the alert status, any events that were throttled, and the response after the alert is triggered.
	How do I check if a scheduled alert failed?
	Since alerts send JSON response payloads, use the json_extract function in the calc operator to filter the results as per the alert status, as follows:
	Step 1: Audit alerts using the following query:
	`audit | where app = "alert"`
	Step 2: Filter the results based on the status of these alert results from Step 1.
	`audit | where app = "alert" | calc status = json_extract(response_digest, "status") | where status = 'FAILED'`
	This query will return all the failed alerts, including the response_digest and request_payload that specifically point out what went wrong in the alert.
	Step 3: Check the alert request payload. For example, this is a cron-based alert:
	`{"alert_id": 2517, "schedule": "* * * * *", "alert_name": "maj test alert", "event_count": "3"}`
	Step 4: Check the response digest. It indicates the provided request URI was invalid (400 Bad Request):
	`{"status": "FAILED", "message": "400 Client Error: Bad Request for url: https://hooks.slack.com/services/T1PC73GUX/B01ZE0/Zzpy96"}`
	How do I check which are the common types of alert failure?
	The following query counts the frequency of all the types of alert failures:
	`audit | where app = "alert" | calc status = json_`

Application	Description

	`extract(response_digest, "status") | where status = 'FAILED'`
	`| calc error_message = json_extract(response_digest, "message")`
	`| aggr count as total_counts by error_message | sort total_counts desc`

search	Captures all the details about different searches, including: • search query • search job ID • total number of results returned and records scanned • Anomali Virtual Compute (AVC) units consumed by the search • total runtime (the amount of time elapsed before getting results) • whether a search was a saved search

`category`

The category of user action that was logged, including api, ui,

`user`

The platform user who initiated the action. This value is the email address of the user.

`action`

Type of the activity recorded, including `create`, `update`, `delete`, `submit_job`, among others. See "Audit Logs for User Actions" on page 364 for more information on the different types of auditable actions.

`client_ip`

IP address of the client that initiates the activity.

`timestamp`

The date and time (local time) the activity was recorded. For example, Mar 13, 2025 17:50:15.000 -07 denotes a search was launced on March 13th at 5:50 PM (UTC-7).

`elapsed_ms`

Total time taken (in milliseconds) to execute the search or API request.

`user_agent`

The user agent of the client that performed the request.

`http_method`

The method used in an HTTP request, such as GET, POST, and so on.

`status_code`

The HTTP status code returned in response to the request.

`search_query`

The query submitted by the user.

For example, `'eventlog | where sourcetype = "ts_onprem" and match (subject,"(ts-[a-z]+|postgresql): FAIL") | fields subject, host'`.

`saved_search_name`

The name of the saved search. This lets you determine which searches are run through search queries in the AQL Search Box and searches that arise from saved searches.

`search_start_time`

Start of the `event_time` time range for the search event, in UNIX timestamp milliseconds (UTC).

`search_end_time`

End of the `event_time` time range for the search event, in UNIX timestamp milliseconds (UTC).

`search_job_id`

The unique ID of a submitted Search job. This is typically a 32-character alphanumeric ID.

`request_uri`

URI of the requested HTTP resource.

`request_payload`

The HTTP request body, in JSON format. You can use it to obtain information about your search. For example, in the following payload:

```
{"origin": "event_search", "total_avc": 0.16}
```

the 'origin' key tells you that the search originated from a event search. Other possible sources of origins are from a dashboard or an alert.

See the AQL calc operator to understand how you can use json_extract to filter your audit results based on the fields in the request body.

`response_digest`

The summary of the response content, typically in JSON format. See the AQL calc operator to understand how you can use the json_extract function to filter your audit results. For example, you can filter down a failed alert using the json_extract function based on the fields in the response, as follows:

```
audit | where app = "alert" | calc status = json_extract(response_
digest, "status") | where status = 'FAILED'
```

This query returns all the failed alerts, an error message that indicates the error in the alert, the total number of events and throttled events.

`request_bytes`

The total size of the request body and headers (in bytes).

`response_bytes`

The total size of the request body and headers (in bytes).

Audit Logs for Analyzing Activity

To analyze user activity through audit logs, use the `audit` keyword in a Anomali Search query. For example, audit logs from the following queries help you examine different user actions in Security Analytics:

Example 1: Check audit logs for export activity.

```
audit

| where category in ('export')

| fields category, action, app, user, client_ip, timestamp, http_
method, request_uri, status_code
```

Example 2: Check audit logs for activity related either to export, saved searches, reports, or dashboards.

```
audit
```

```
| where category in ('export', 'saved_search', 'report',
'dashboards')

| fields category, action, app, user, client_ip, timestamp
```

Example 3: Check audit logs for actions that involved queuing.

```
audit

|  where action contains_ci "queue"
```

Example 4: Check audit logs for activity related either to multiple user actions across different Anomali features.

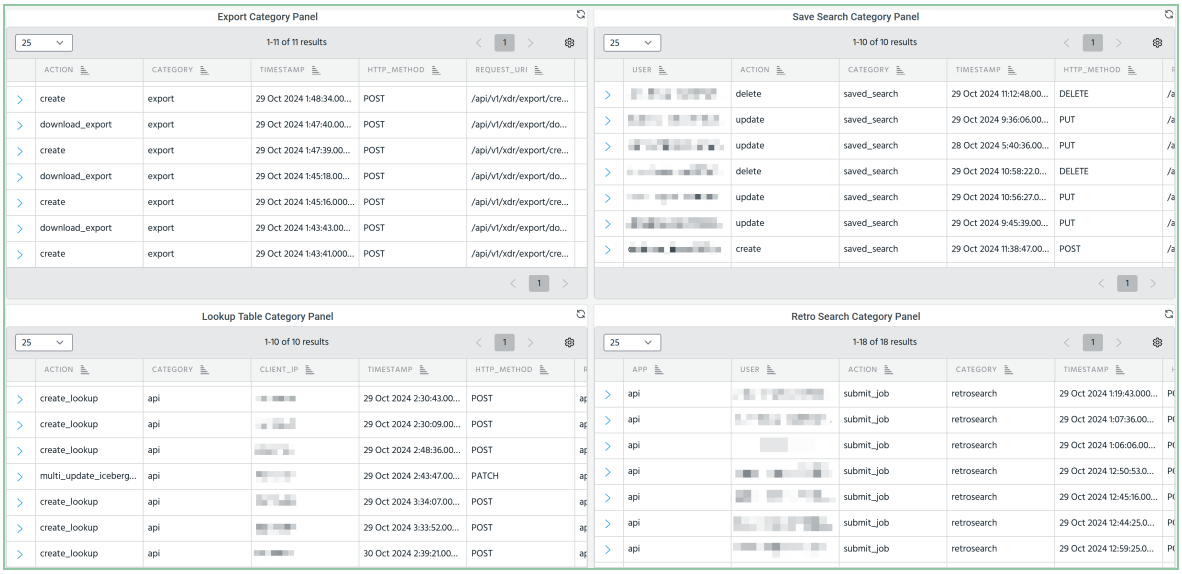
```
audit

| where category in ("search", "saved_search", "alerter_config",
"retrosearch", "excludelist", "report", 'api', 'export')

| fields category, action, user, client_ip, timestamp, http_
method, request_uri, status_code, request_payload
```

Note: `api` is the category for a user action that indexes against a lookup table.

Creating Dashboards for Audits



To simplify the process of examining audit logs, Anomali recommends you create an audit dashboard that contains dashboard panels dedicated to the fields scoped in "Auditing Scope" on page 355.

To create an audit log dashboard:

1. Go to Anomali Search homepage.
2. Enter a valid query using the `audit` operator. For example, the following query returns audit logs for all the users that issued a retrospective search:

```
audit
| where category in ('retrosearch')
| fields user, action, timestamp
```

3. Switch to the Visualization tab under the Search Box.
4. Add the suggested visualization to your dashboard as a dashboard panel. See Working with Visualizations for more information on how you can configure the panel.
5. Repeat steps 1-4 to add a panel for each of the applications in your audit log dashboard.

Audit Logs for User Actions

The following tables list all the user actions that are included in audit logs:

Alert Configuration Audit Logs

User Actions in Managing Alerts	Descriptions
`action=Add new alert rule`	The user created a new alert.
`action=Enable alert rule`	The user enabled an alert that was either newly-created or previously disabled.
`action=Disable alert rule`	The user disabled an alert and therefore prevents it from firing.
`action=Edit alert rule`	The user changed an alert configuration.
`action=Delete alert rule`	The user deleted an alert.

Saved Searches Audit Logs

User Actions in Searches	Descriptions
`action=Delete saved activity`	The user deleted a saved search.
`action=Save activity`	The user defined a search query in Activity and saved it.
`action=Update activity`	The user updated a saved search.

Retrospective Searches Audit Logs

User Actions in Conducting Retrospective Searches	Descriptions
`action=Create new retrospective search configuration`	The user created and saved a new retrospective search on the Activity page.

User Actions in Conducting Retrospective Searches	Descriptions
`action=Update retrospective search configuration`	The user updated configuration of an existing retrospective search.
`action=Delete retrospective search configuration`	The user deleted a retrospective search.

Report Management Audit Logs

User Actions in Managing Reports	Descriptions
`action=Delete report job`	The user deleted a report that was previously added to the **Manage** > **Reports** > **Jobs** tab.
`action=Schedule report job`	The user created a report schedule.
`action=Update report job`	The user updated a scheduled report setting.
`action=Enable report job`	The user enabled a report so that it runs according to schedule.
`action=Disable report job`	The user disabled a report and therefore the report is not running.

Export Audit Logs

User Actions in Exports	Descriptions
`action=Create export job`	The user created and saved an export configuration, for example, search results, into a desired format (JSON or CSV).
`action=Delete export job`	The user deleted a saved export job.
`action=Delete group of export job`	The user deleted multiple export jobs.
`action=Download export file`	The user downloaded an exported file.

Lookup Table Audit Logs

User Actions in Lookup Table Configurations	Descriptions
`action=Add New lookup table`	The user created a new lookup table in Settings > Lookup Tables.
`action=Edit lookup table`	The user edited an existing lookup table.
`action=Delete lookup table`	The user deleted a lookup table.
`action=Upload local CSV for lookup table`	The user uploaded a CSV file to be used as a lookup table. File is stored in `<Anomali Security Analytics installation> /external/properties`.

Exclude List Audit Logs

User Actions in Managing Exclude Lists	Descriptions
`action=Upload ioc excludelist`	The user uploaded an IOC exclude list.
`action=Upload dga excludelist`	The user uploaded a DGA exclude list.
`action=Upload asset excludelist`	The user uploaded an asset exclude list.
`action=Suppress indicator`	The user marked a matched indicator on search results as suppressed.
`action=Remove ioc excludelist`	The user removed a suppressed indicator from the list.

User Actions in Managing Exclude Lists	Descriptions
`action=Remove asset excludelist`	The user removed an asset from the list.
`action=Add to dga excludelist`	The user added a DGA match to the list.
`action=Remove dga excludelist`	The user deleted a domain from the list.

Audit Logs for Dashboard updates

User Actions in Dashboards	Descriptions
`action=Create dashboard`	The user creates a new dashboard or clones an existing dashboard.
`action=Update dashboard`	The user updates an existing dashboard.
`action=Delete dashboard`	The user deletes an existing dashboard.

Chapter 9: Data Onboarding and Log Source Management

Anomali Security Analytics supports log ingestion from various telemetry log sources. This event telemetry data can be ingested in one of the following ways:

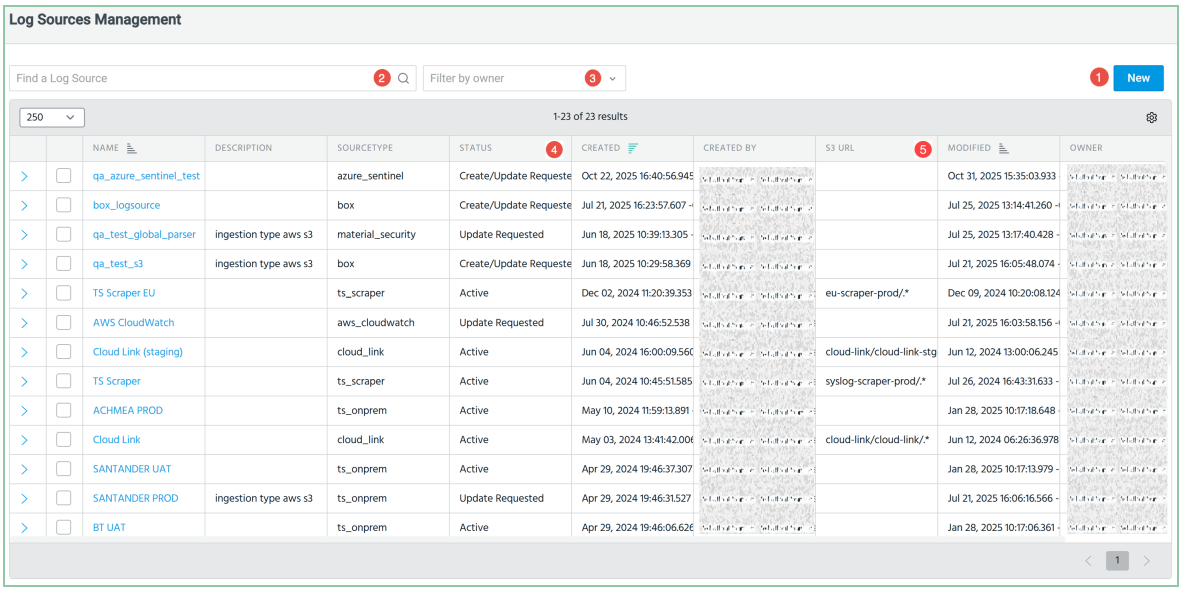
- **Log forwarders**: Anomali recommends using log forwarders such as NXLog or Cribl to ship event data to an AWS S3 bucket that you share with Anomali.
- **API calls**: Cloud-to-Cloud services allow Anomali to make API calls and directly fetch your data for ingestion.
- **Universal Link**: Some log sources depend on Universal Link for data ingestion.

See Supported Log Sources for the complete list of log sources Anomali currently supports.

Onboarding your data

> **Note:** See Anomali Search Data Retention Policy to understand how your data is retained over time in the Anomali platform.

As an org admin, you can onboard your data by adding a log source in Anomali Search by navigating to **Search** > **Manage** > **Log Sources**.



1	Add new log source: Click **New** to add a new log source. See Supported Log Sources for the complete list of log sources Anomali currently supports. For each log source, as an org admin, you can select: • **Ingest Method**: The method you use to ingest your event data logs into Anomali. ▪ AWS S3: Configure AWS S3 bucket and provide its AWS SQS Queue URL, AWS Acces Key ID, Secret Access Key, along with the S3 key path. ▪ API: Uses an API token to make API calls and collect event log data for ingestion. • **Permissions**: Set Private or Shared read-write permissions for a role mapped to a user group or an entire organization.
2	Find a log source: Search and select a log source from the table of log sources.

3	Filter by owner: You can filter log sources by owner. Possible values include: • **Mine**: returns log sources for which you are the owner. • **<user>**: returns log sources where the selected user is the owner.

4	Status of log source: The Status column denotes the current status of a log source, from creating a log source to confirming its deletion. Possible statuses include:
	• **Create Requested**: When you add a log source. You will also receive an email confirmation, with a copy sent to Anomali.
	• **Active**: The log source is now `Active` after it's either been created or updated and after Anomali has successfully confirmed the ingestion. Your data is now ready for analysis within the Anomali platform. An email confirmation confirms this change.
	• **Update Requested**:
	  ▪ Once you submit a request to update your log source, you will receive an email confirmation, with a copy sent to Anomali.
	  ▪ `Update Requested` is also the status when you successfully complete a pending action requested by Anomali.
	• **Deletion Requested**: You would like to delete a log source. The deletion will be complete once Anomali has confirmed the deletion.
	• **Inactive**: The log source is now `Inactive` after Anomali has completed its deletion.
	Here are 3 common scenarios for status changes:
	Scenario 1: `Create Requested` > `Active`.
	Scenario 2: `Create/Update Requested` OR `Update Requested` > `Active`.
	Scenario 3: `Deletion Requested` > `Inactive`.

5	S3 URL: URL to the S3 path from which the data is to be ingested.

Security Analytics Best Practices

Use the recommendations below to optimize the overall resource utilization.

Limit Cloud Link file size

To ensure optimal performance from Cloud Link for event telemetry ingestion, Anomali recommends that you limit the telemetry file sizes as follows:

- Minimum compressed file size: 1 MB
- Maximum compressed file size: 50 MB

> **Note:** Anomali recommends you compress your telemetry data files prior to the file ingestion.

Supported Log Sources (Limited Availability)

Anomali supports many log sources, using either AWS S3, Universal Link, or API calls for data ingestion. See Eventlog Schema to understand all the event log fields that Anomali captures from varied event log sources and correspondingly maps them in the Anomali Security Analytics eventlog schema.

Supported log sources

> **Note:** * denotes a log source that depends on Universal Link for log ingestion.

- 1Password
- Absolute
- Ad Password Interceptor
- Aisera
- Akamai SIEM
- Algosec
- Alkira
- AppViewX
- Aruba Clearpass
- Aruba Networks
- Asana
- Athoc
- Auth0
- AVI Networks
- AWS Autoscaling

- AWS CloudTrail
- AWS CloudWatch
- AWS Config Notification
- AWS EC2
- AWS GuardDuty
- AWS Health
- AWS SSM
- AWS VPC DNS
- AWS VPC Flow
- AWS WAF
- Bitwarden
- Bomgar
- Box
- Canarytools Audit
- Canarytools Device
- Canarytools Incident
- Canarytools Token
- Canarytools User
- Carbon Black
- Catalina
- Cisco ACS
- Cisco ASA
- Cisco ESA Amp

- Cisco ESA AntiSpam
- Cisco ESA Antivirus
- Cisco ESA Authentication
- Cisco ESA Bounce
- Cisco ESA CLI Audit
- Cisco ESA Greymail
- Cisco ESA HTTP
- Cisco ESA LDAP
- Cisco ESA NTP
- Cisco ESA Quarantine GUI
- Cisco ESA Reporting
- Cisco ESA Scanning
- Cisco ESA Textmail
- Cisco FTD
- Cisco Ironport
- Cisco ISE
- Cisco Meraki
- Cisco Router
- Cisco Switch
- Cloudflare DNS
- Cloudflare WAF
- Crowdstrike Event Streams
- Crowdstrike FDR

- Custom *
- Cyberark Audit
- Cyberark EPV
- Docker
- Dropbox
- Duo
- Envoy
- ESXi
- F5 BIG-IP
- F5 BIG-IP TCL Error
- Falcon Filevantage
- Falcon Threat
- Falcon Vulnerability
- Fastly
- Fluentd
- Forcepoint
- Fortinet (Ingestion possible through Cloud Link and Universal Link)
- Generic Syslog *
- GCP Auto
- GCP Firewall
- GCP VPC
- GitHub Cloud
- Gitlab

- Google SecOps
- Google Workspace
- Guardicore Centra
- HA Proxy
- Heroku
- IAM Cyberark AppAudit
- IAM Cyberark AppConsole
- IBM QRadar
- IBM QRadar OnPrem *
- IdentityIQ
- IIS
- Imperva WAF
- Infoblox Audit
- Infoblox File
- Infoblox DHCP
- Infoblox DNS
- JAMF
- JumpCloud
- Juniper Corero
- Juniper JUNOS
- Juniper Switches
- Kafka *
- Lacework

- LeapXpert
- Linux Audit
- Linux Auth
- MacOS
- Material Security
- Microsoft Active Directory
- Microsoft Azure Active Directory
- Microsoft Azure Sentinel
- Microsoft Cluster Services Audit
- Microsoft Cluster Services Azure
- Microsoft Defender
- Microsoft Defender ATP
- Microsoft DHCP
- Microsoft Graph Security Alert
- Microsoft Office365
- Microsoft Office365 Activity Reports
- Microsoft Office365 Device Management
- Microsoft Office365 Graph
- Microsoft Office365 Identity Access Report
- Microsoft Office365 Identity Protection
- Microsoft Office365 Management Activity
- Microsoft Office365 Service Communication
- Microsoft Office365 Usage Report

- Mimecast Version 2.0
- Mimecast Version 1.0
- Miro Audit
- Nametag
- Nasuni Log
- Nasuni Storage
- NetFlow *
- Netskope
- Not Listed
- Notion
- NXLog Agent
- Obsidian
- Okta
- Okta Agent
- Okta Radius
- Okta Radius Access
- Oracle IAM Access
- Oracle IAM Errors
- Oracle IAM Replication
- Oracle VCN Flow
- PagerDuty
- Palo Alto Networks Firewall
- PeopleSoft

- Postfix
- Proofpoint
- PRTG
- Rapid7
- RSA NetWitness *
- Rubrik
- Secure Relay
- ServiceNow
- sFlow *
- Sophos
- Suricata
- Suricata (OnPrem to Cloud) *
- Sumo Logic
- Symantec ICDx *
- Tanium HTTP
- Teleport
- Tenable AD Alerts
- Thycotic
- Windows
- Windows Event
- Winlogbeat *
- Wiz
- Workday

- Zeek
- Zoom
- Zscaler Audit
- Zscaler DNS
- Zscaler FW
- Zscaler Web
- Zscaler LSS Web
- Zscaler LSS ZPA App
- Zscaler LSS ZPA Auth

1Password

Anomali supports the ingestion of 1Password logs through the 1Password Events API and AWS S3.

Events API

You can use your existing API token or create a new token to add a new log source in the Anomali platform.

Onboarding steps

Step 1: Create API token

To create an API token:

1. Sign into your 1Password account.
2. Click **Integrations** > **Directory** > **Events Reporting**.
3. Click **Other** to initiate integration with Anomali.
4. Enter a name for the integration and click **Add integration**.
5. Enter a name, an expiry date, and event types permitted for the token, then click **Issue token**.Securely store the token value for the subsequent steps.

Step 2: Add 1Password as a new log source

To add 1Password as a new log source on the Anomali platform:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select **1Password** as the source type.
6. Select **API** as the ingestion method.
7. Select AWS S3 as the ingest method.
8. Provide the Basic Configuration details:

a. **Server**: Enter the server name.

b. **Token**: Enter your existing token ID or the new token you created in "Step 1: Create API token" on the previous page.

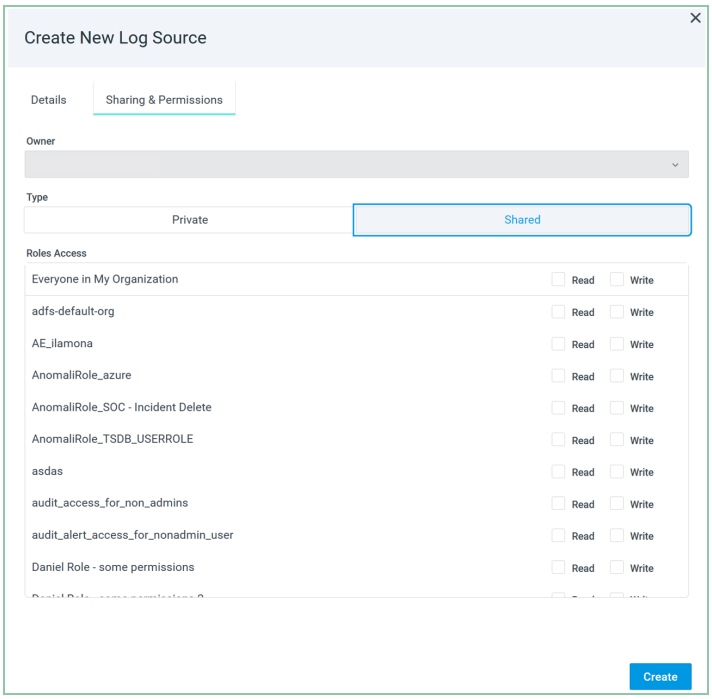
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 3: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.

2. Type: Select the type of permission assigned to the view:

a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.

b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 4: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 5: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

AWS S3

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

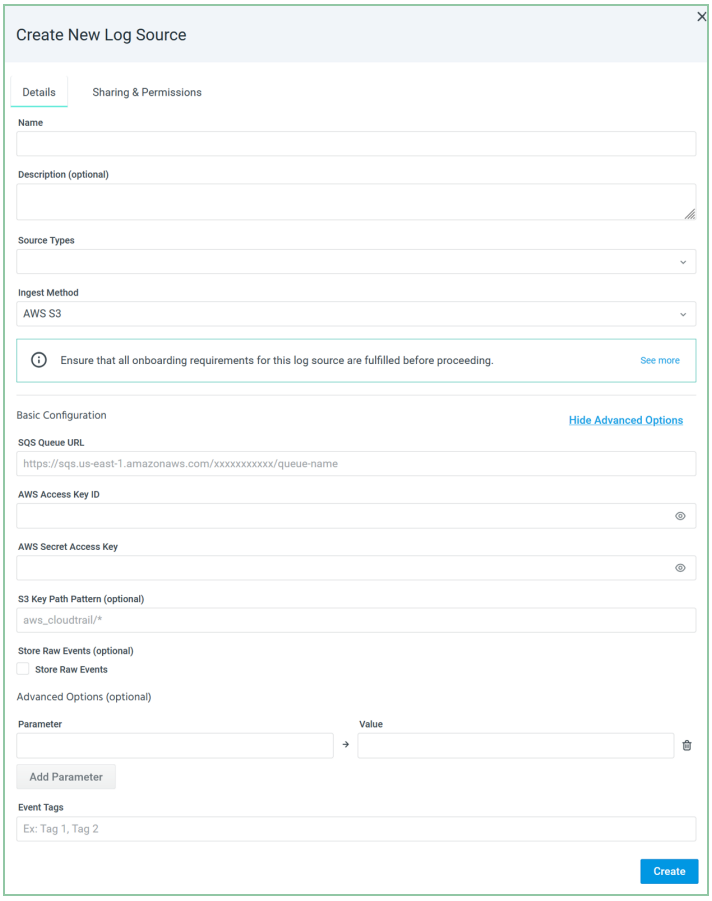
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add 1Password as new log source



On the Anomali platform, add 1Password as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `1password/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"1password"` or `"1password_sourcetype"` are correct, however `"1password sourcetype"` is incorrect.

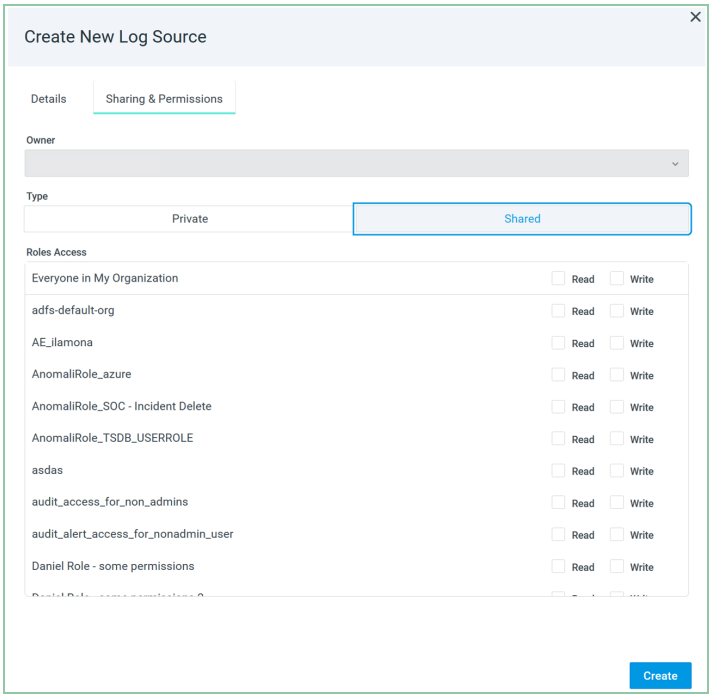
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create`

`Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Absolute

Anomali supports the ingestion of Absolute logs. The following article explains the steps you must complete to ingest Absolute logs into Anomali.

Onboarding steps

Prerequisites

You must have admin privileges to create access token.

Step 1: Create Access Token

1. Sign in to your Absolute platform.
2. Navigate to **API Token Management**.
3. Click **Create New API Token**.
4. (Optional) Provide a descriptive name for the token.
5. Click **Save**.

Step 2: Add Absolute as new log source

To add Absolute as a new log source on the Anomali platform:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select **Absolute** as the source type.
6. Select **API** as the ingestion method.
7. Select API as the ingest method.
8. Provide the Basic Configuration details:
    a. **Token ID**: Enter the token ID of the access token from "Step 1: Create Access Token" above.

b. **API URL**: Enter the account access key you obtained in "Absolute " on the previous page.

c. **Wildcard Log Schema**: Provide the wildcard log schema.

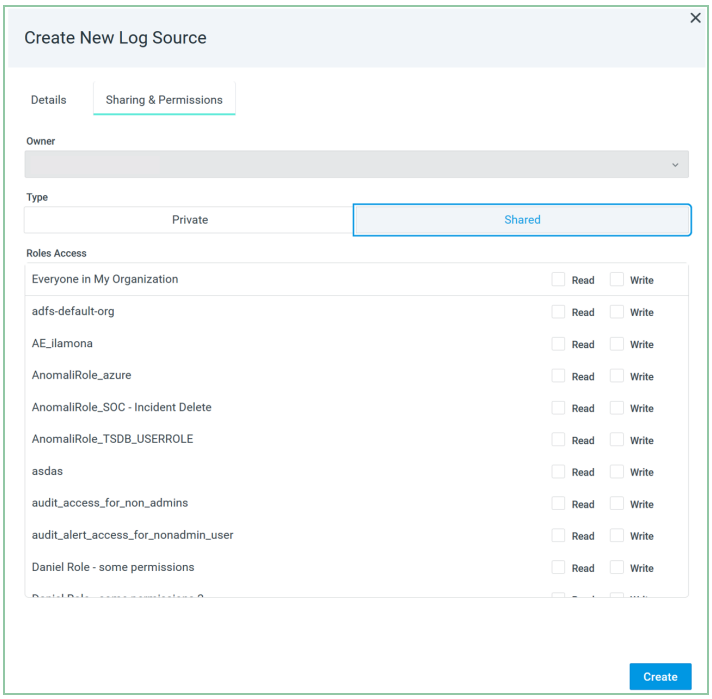
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 3: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.

2. Type: Select the type of permission assigned to the view:

a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.

b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 4: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 5: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Ad Password Interceptor

Anomali supports the ingestion of Ad Password Interceptor logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

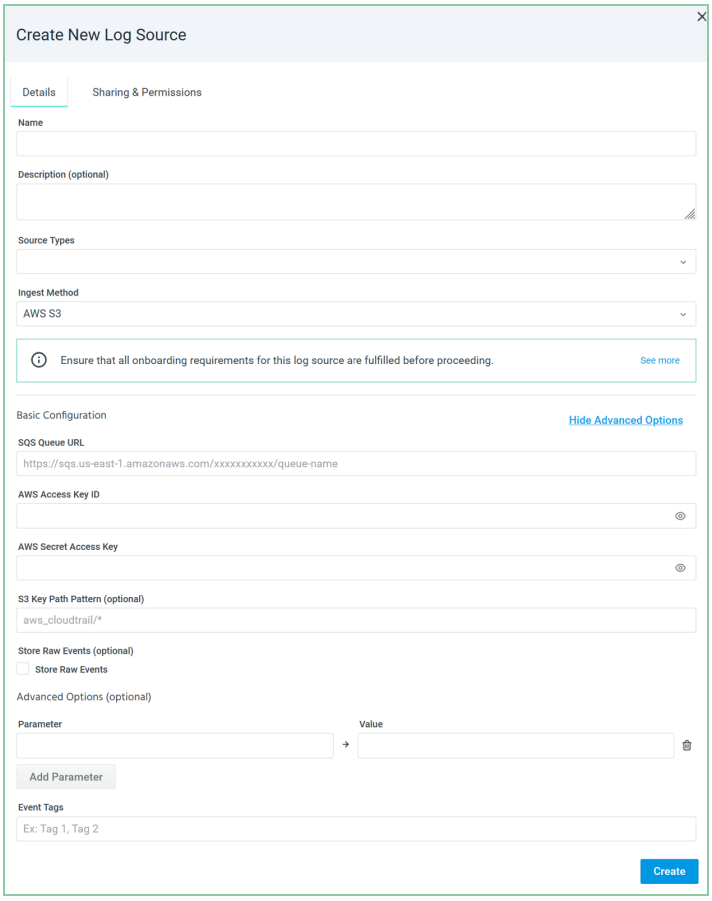
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Ad Password Interceptor as new log source



On the Anomali platform, add Ad Password Interceptor as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `ad_password_interceptor/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"ad_password_interceptor"` is correct, however `"Ad Password Interceptor"` is incorrect.

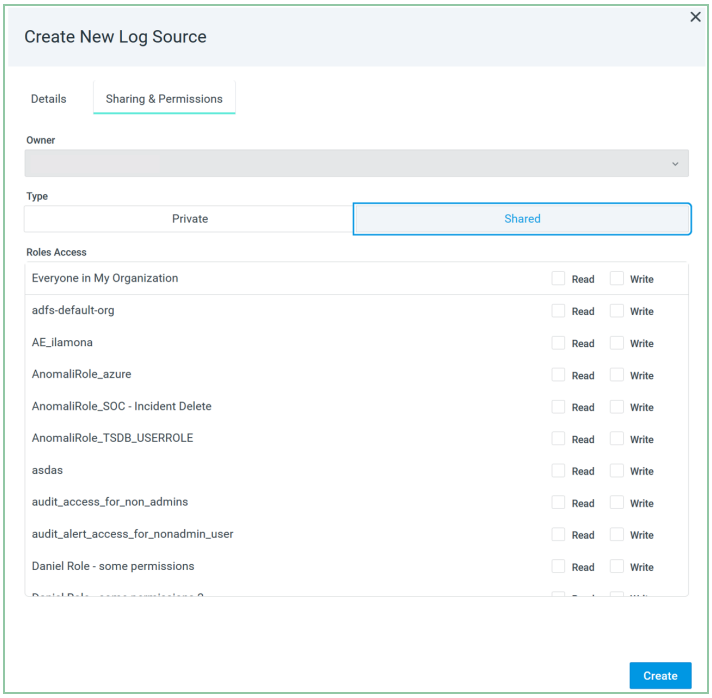
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Aisera

Anomali supports the ingestion of Aisera logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

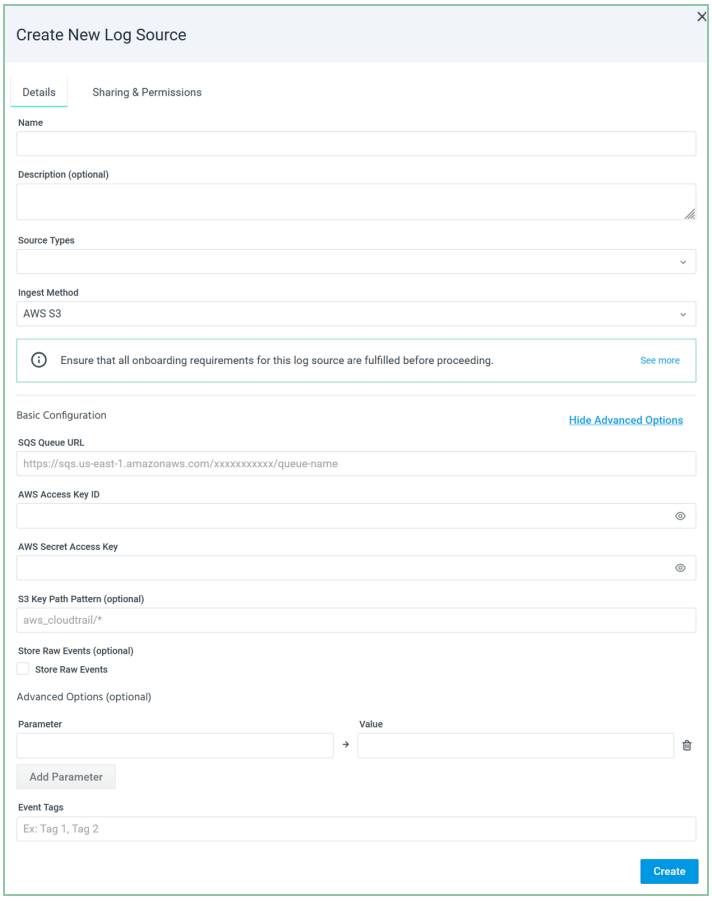
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Aisera as new log source



On the Anomali platform, add Aisera as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `aisera/year=2025/month=03/day=22/events/event_data_logs/`.

- Sourcetype name must not contain any spaces: For example, `"aisera"` or `"aisera_sourcetype"` are correct, however `"aisera sourcetype"` is incorrect.

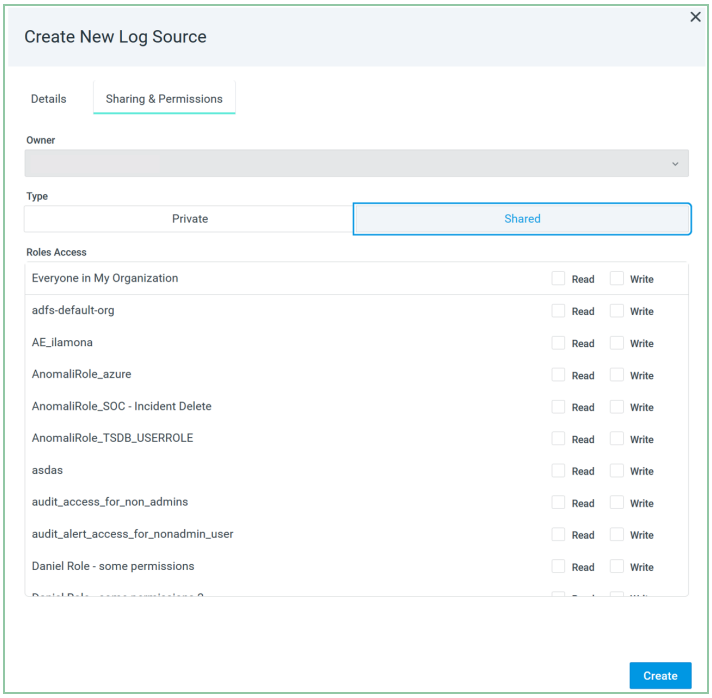
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Akamai SIEM

Anomali supports the ingestion of Akamai SIEM logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

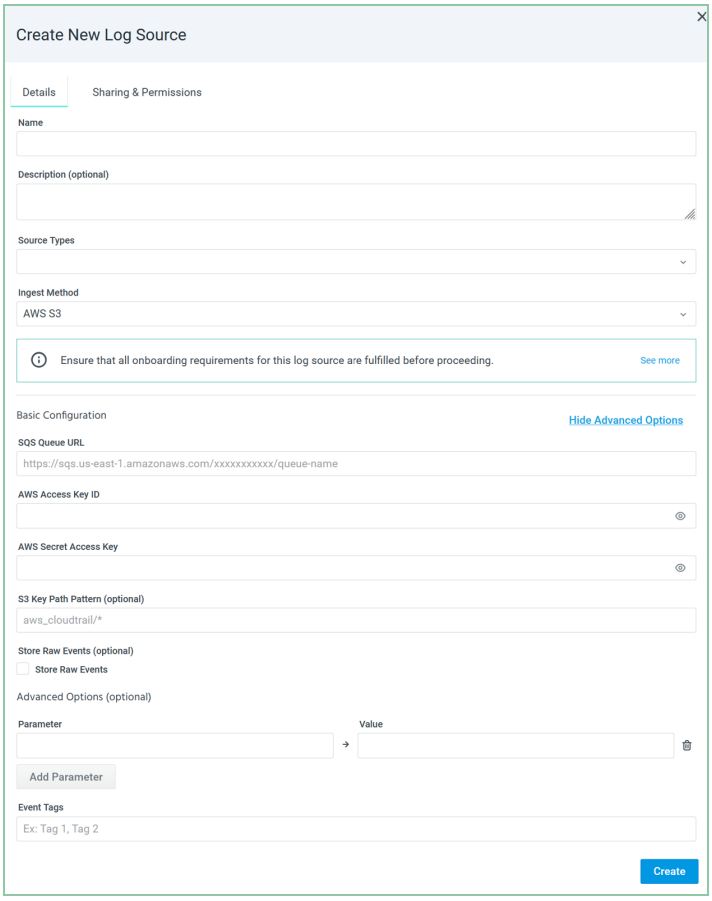
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Akamai SIEM as new log source



On the Anomali platform, add Akamai SIEM as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `akamai_siem/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"akamai_siem"` is correct, however `"akamai siem"` is incorrect.

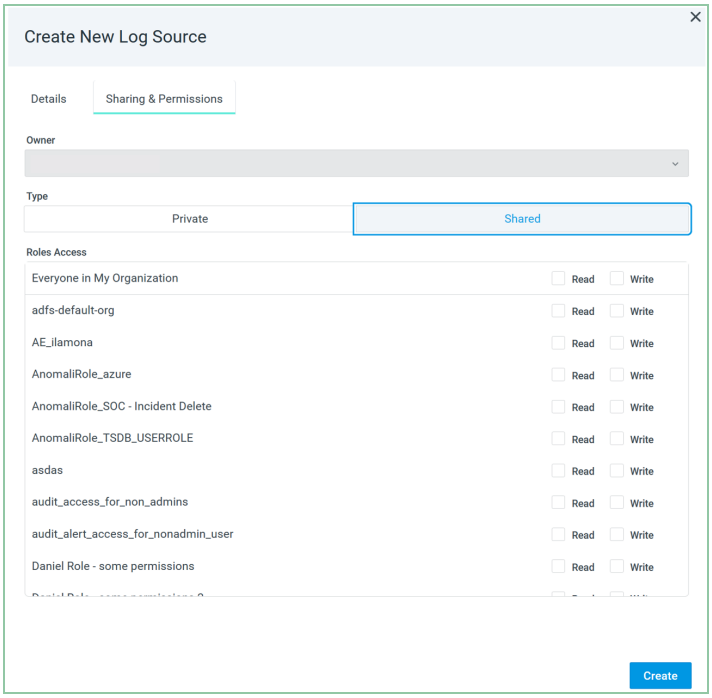
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Algosec

Anomali supports the ingestion of Algosec logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

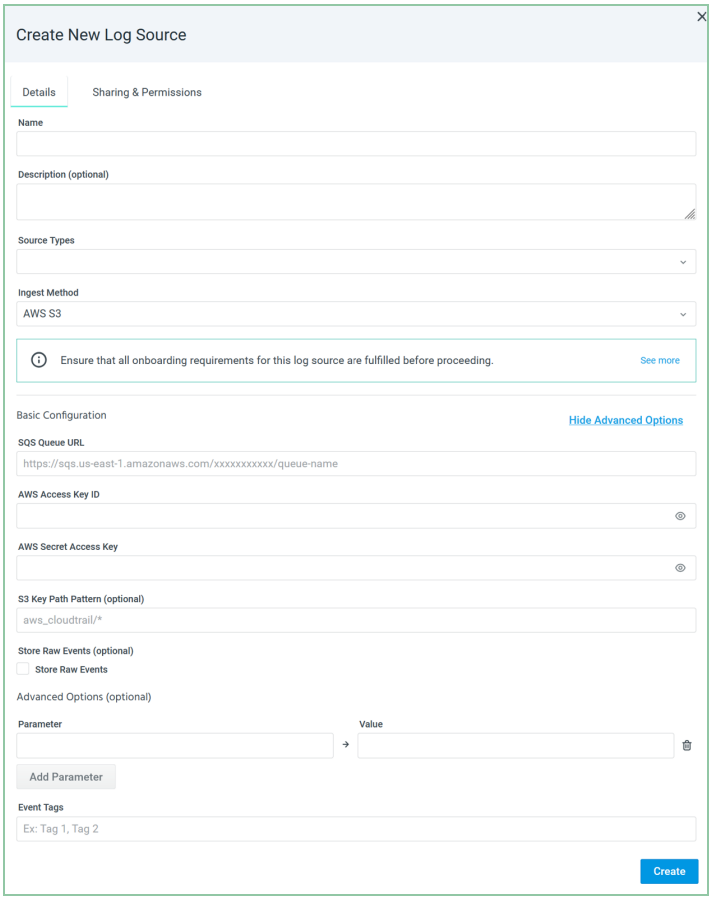
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Algosec as new log source



On the Anomali platform, add Algosec as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `algosec/year=2025/month=03/day=22/events/event_data_logs/`.

- Sourcetype name must not contain any spaces: For example, `"algosec"` or `"algosec_sourcetype"` are correct, however `"algosec sourcetype"` is incorrect.

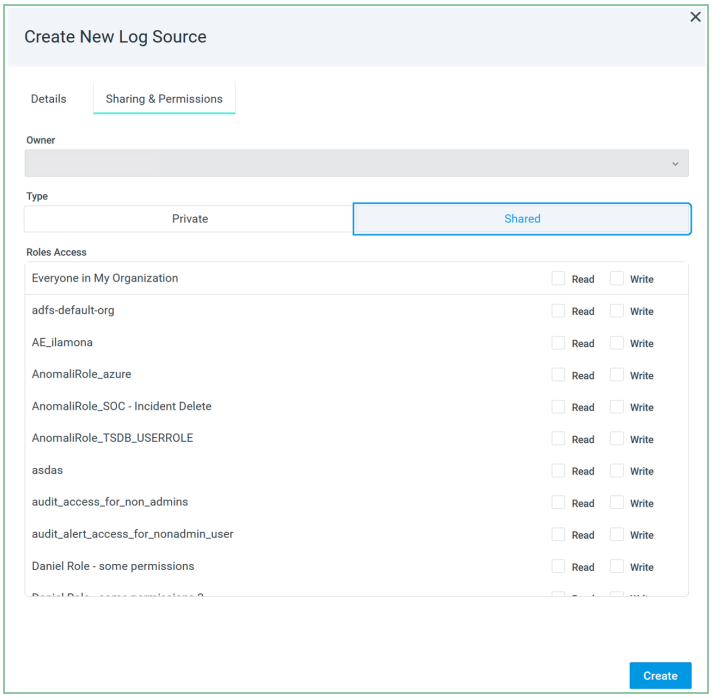
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

AppOmni

Anomali supports the ingestion of AppOmni logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

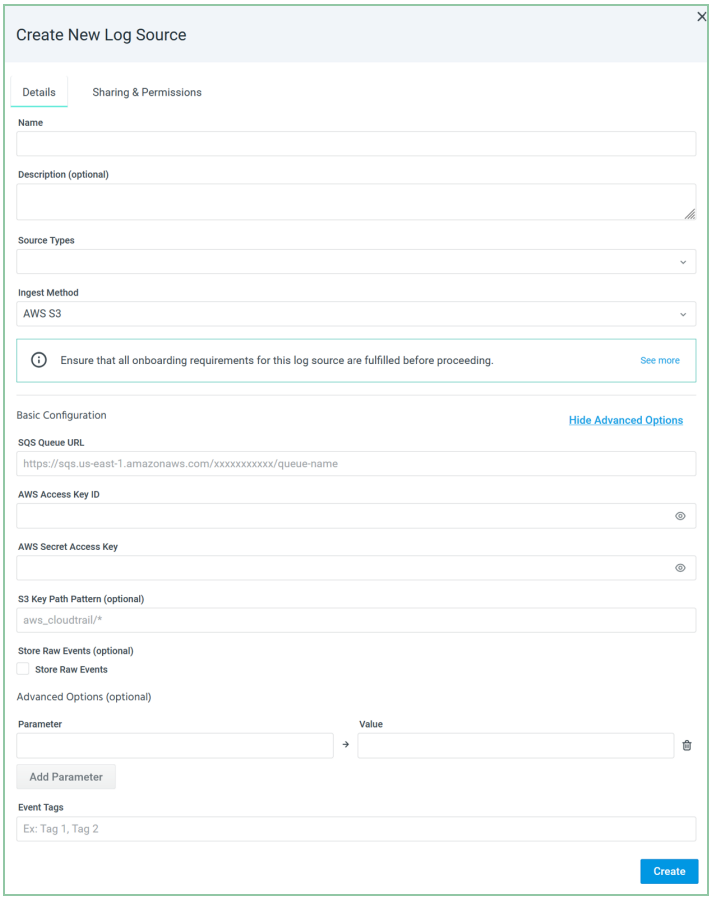
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add AppOmni as new log source



On the Anomali platform, add AppOmni as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `appomni/year=2025/month=03/day=22/events/event_data_logs/`.

- Sourcetype name must not contain any spaces: For example, `"appomni"` is correct, however `"appomni"` is incorrect.

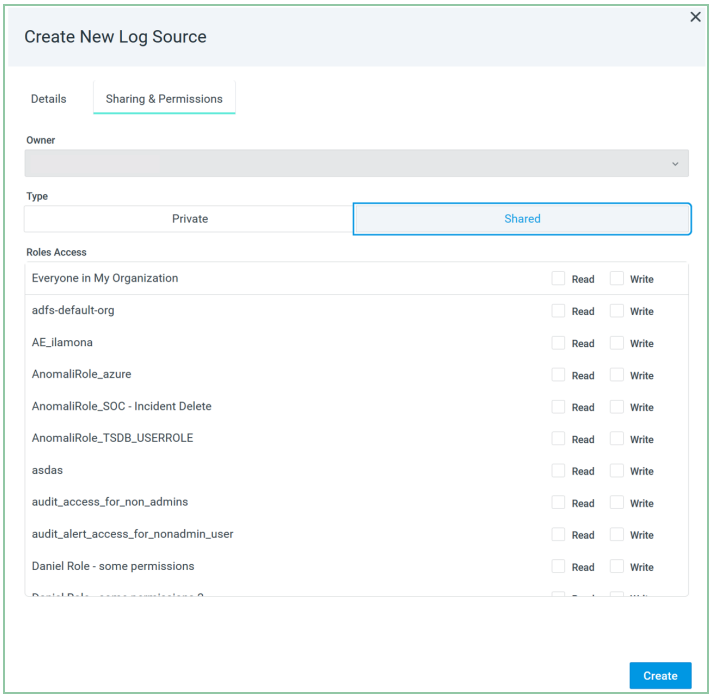
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

AppViewX

Anomali supports the ingestion of AppViewX logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

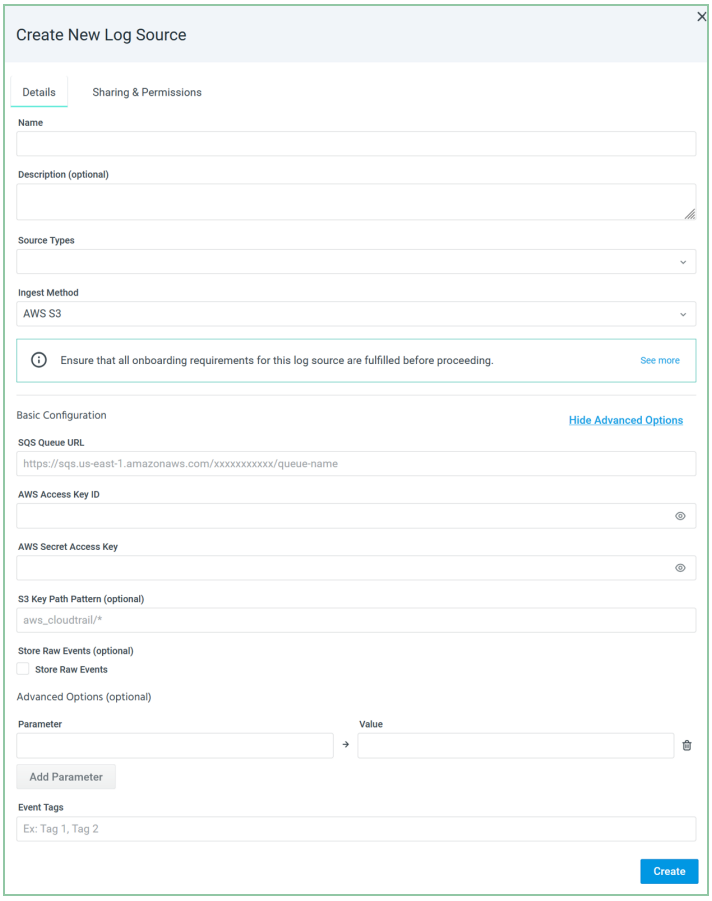
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add AppViewX as new log source



On the Anomali platform, add AppViewX as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `appviewx/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"app_viewx"` or `"appviewx_sourcetype"` are correct, however `"appviewx sourcetype"` is incorrect.

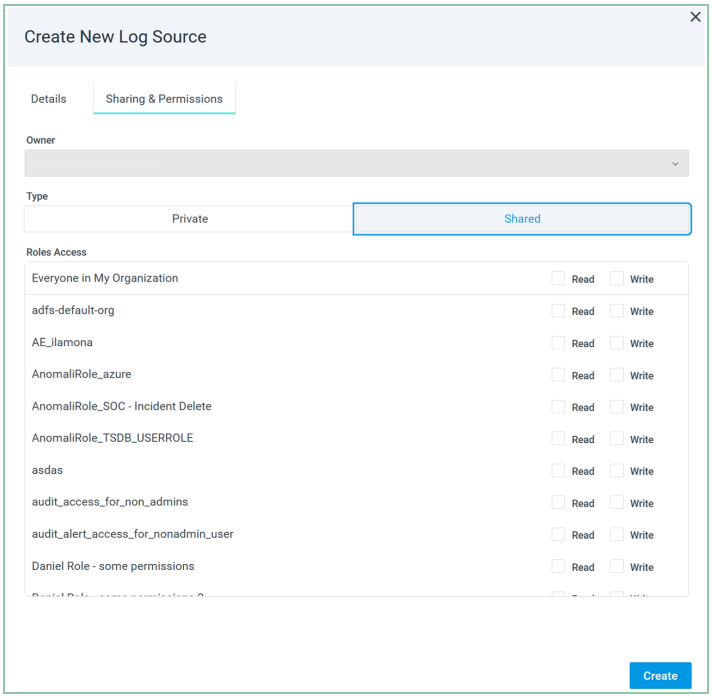
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Aruba Clearpass

Anomali supports the ingestion of Aruba Clearpass logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

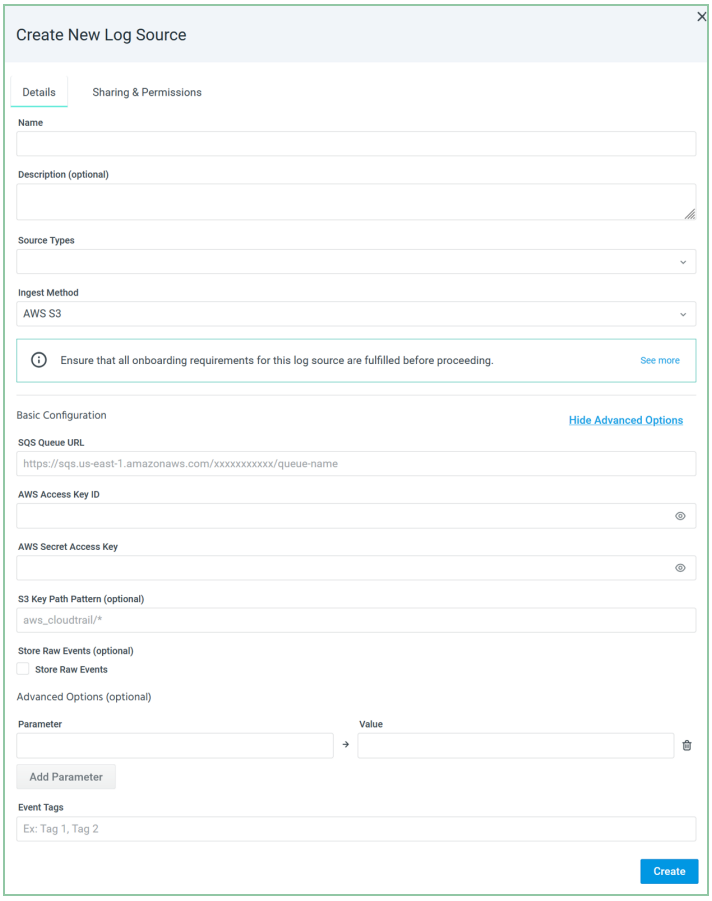
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Aruba Clearpass as new log source



On the Anomali platform, add Aruba Clearpass as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `aruba_clearpass/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"aruba"` or `"aruba_clearpass"` are correct, however `"Aruba Clearpass"` is incorrect.

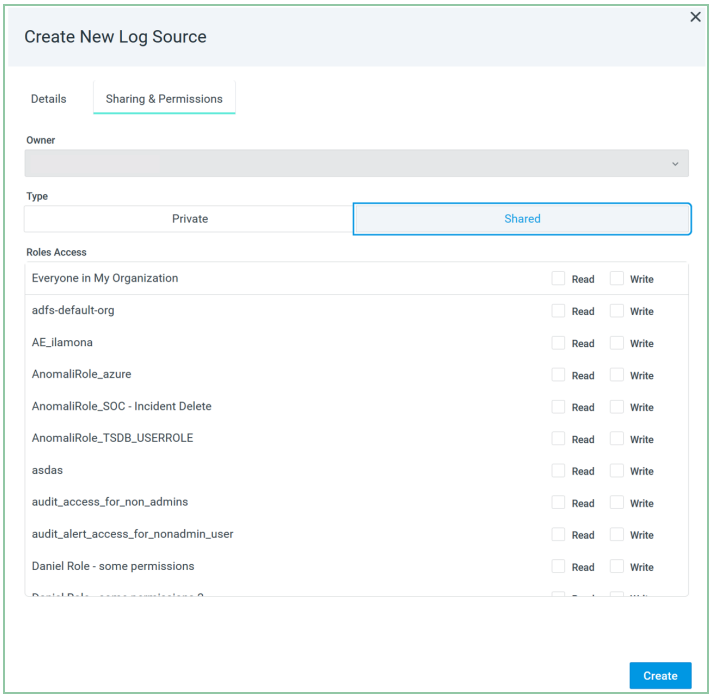
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Aruba Networks

Anomali supports the ingestion of Aruba Networks logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

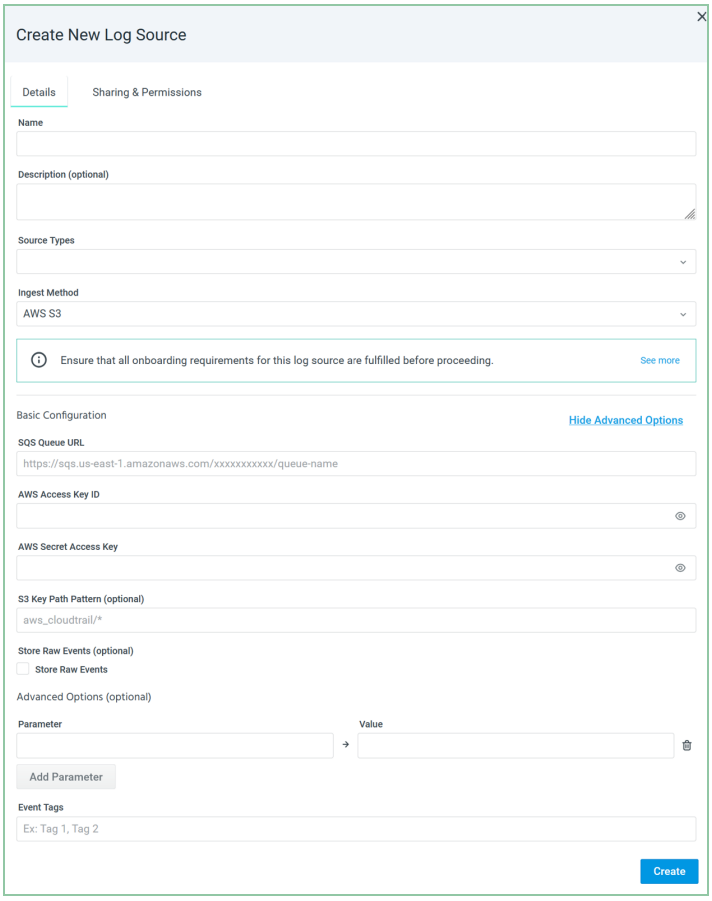
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Aruba Networks as new log source



On the Anomali platform, add Aruba Networks as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `aruba_networks/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"aruba"` or `"aruba_networks"` are correct, however `"Aruba Networks"` is incorrect.

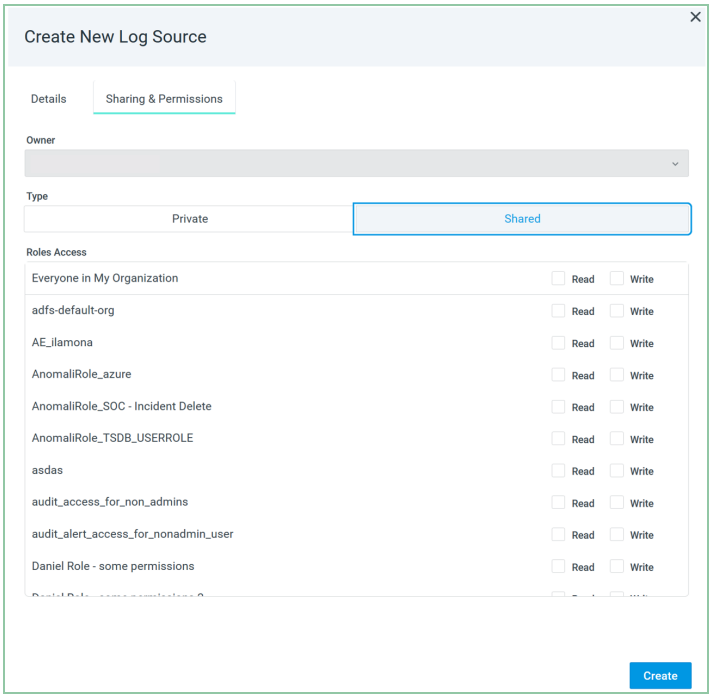
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

AVI Networks

Anomali supports the ingestion of AVI Networks logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

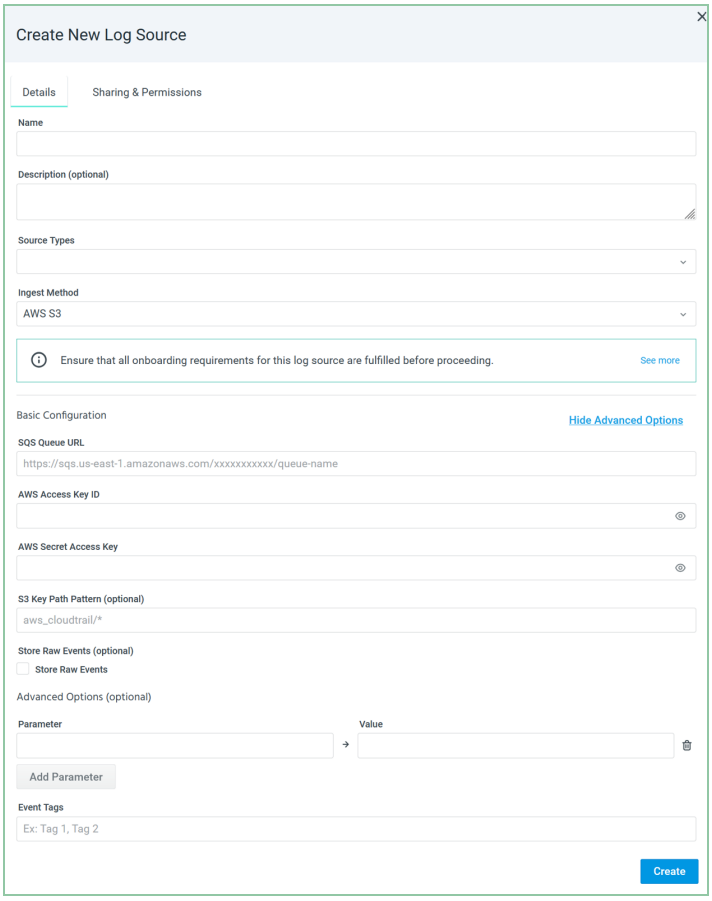
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add AVI Networks as new log source



On the Anomali platform, add AVI Networks as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `avi_networks/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"avi_networks"` is correct, however `"avi networks"` is incorrect.

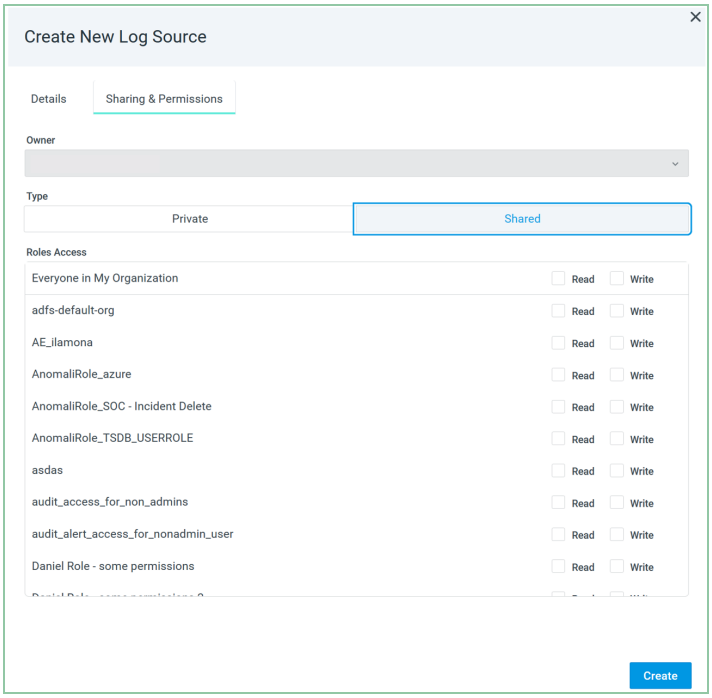
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

AWS Autoscaling

Anomali supports the ingestion of AWS Autoscaling logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

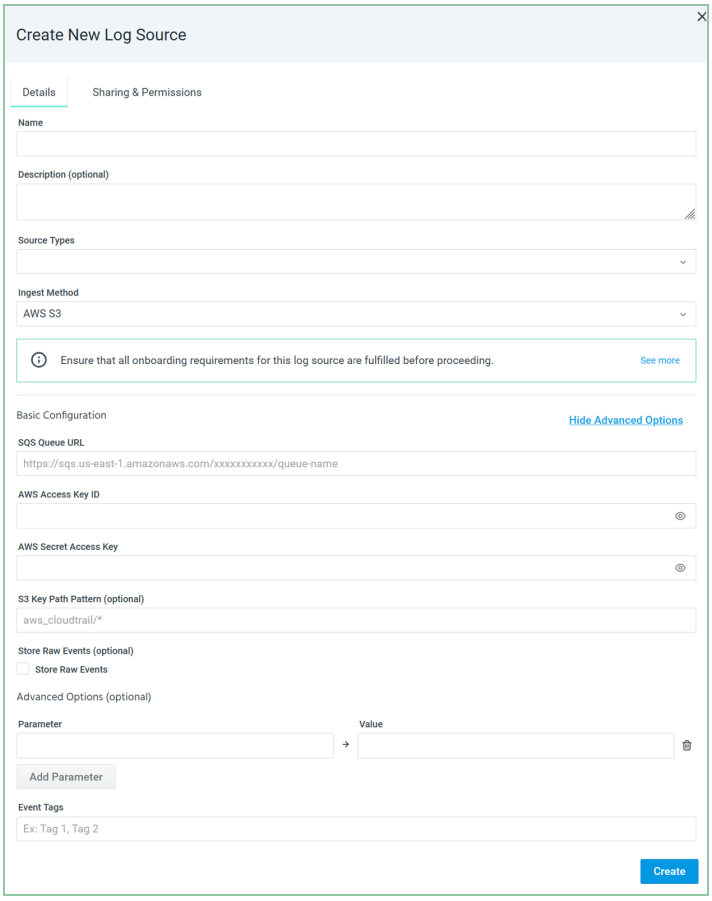
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add AWS Autoscaling as new log source



On the Anomali platform, add AWS Autoscaling as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `aws_autoscaling/year=2025/month=03/day=22/events/event_data_logs/`.

- Sourcetype name must not contain any spaces: For example, `"aws_autoscaling"` is correct, however `"AWS Autoscaling"` is incorrect.

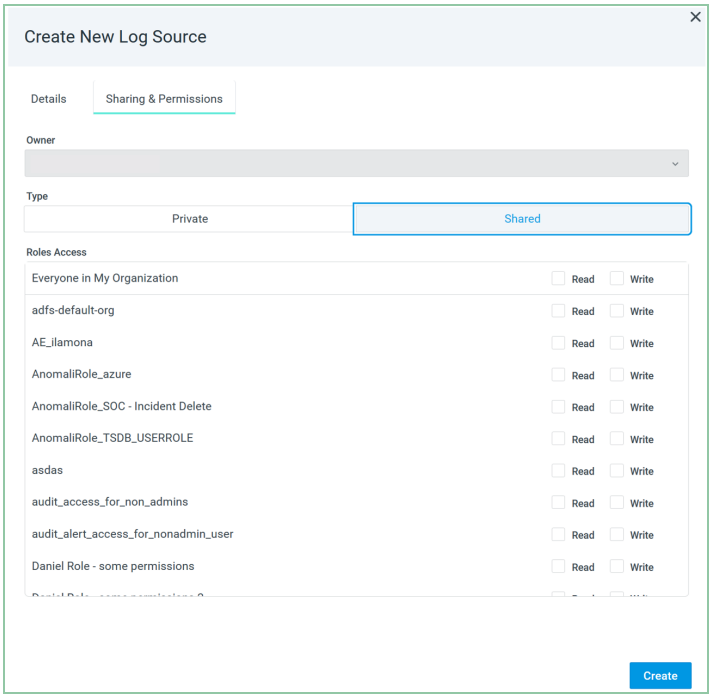
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

AWS CloudTrail

Anomali supports the ingestion of Amazon Web Services (AWS) CloudTrail logs stored in your AWS S3, using Amazon Simple Queue Service (SQS) for notifications.

Once S3 event notifications are configured to send updates to the SQS queue you designate, Anomali automatically pulls the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

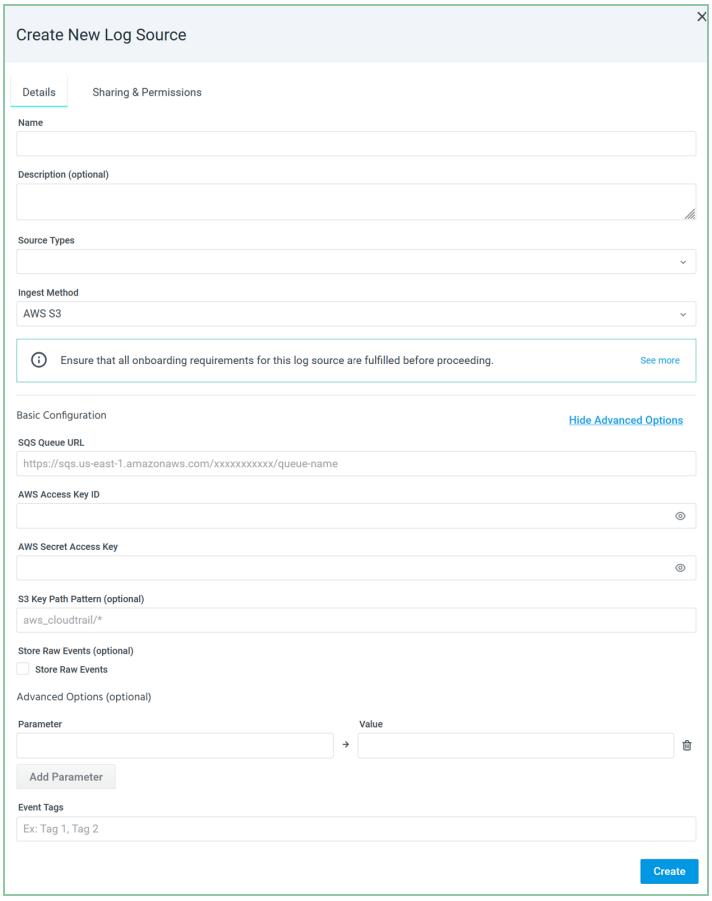
Step 1: Set up SQS queue

To send CloudTrail logs to Anomali, you will first need to set up an Amazon SQS queue.

Step 2: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 3: Add CloudTrail as new log source



On the Anomali platform, add CloudTrail as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on the previous page for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `aws_cloudtrail/year=2025/month=03/day=22/events/event_data_logs/`.

- Sourcetype name must not contain any spaces: For example, `"aws_cloudtrail"` is correct, however `"aws cloud trail"` is incorrect.

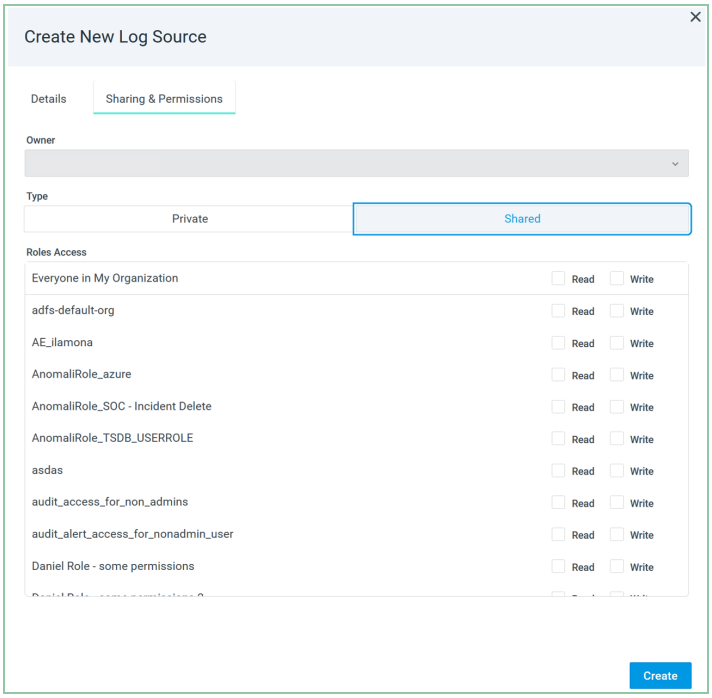
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 4: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 5: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 6: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

AWS CloudWatch

Anomali supports the ingestion of Amazon Web Services (AWS) CloudWatch logs stored in your AWS S3, using Amazon Simple Queue Service (SQS) for notifications.

Once S3 event notifications are configured to send updates to the SQS queue you designate, Anomali automatically pulls the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

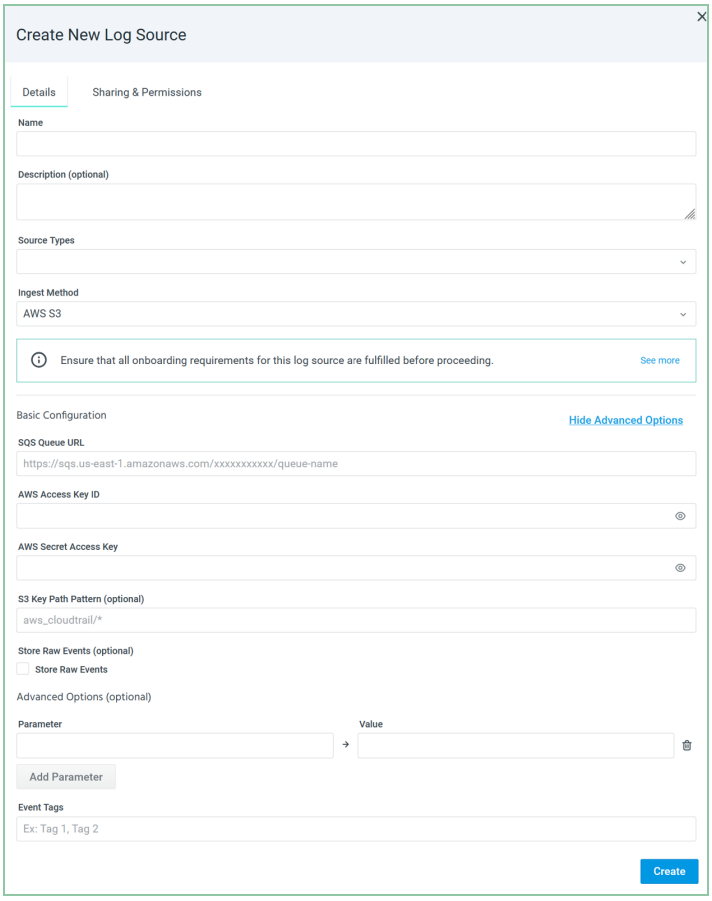
Step 1: Set up SQS queue

To send CloudWatch logs to Anomali, you will first need to set up an Amazon SQS queue.

Step 2: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 3: Add CloudWatch as new log source



On the Anomali platform, add CloudWatch as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `aws_cloudwatch/year=2025/month=03/day=22/events/event_data_logs/`.

- Sourcetype name must not contain any spaces: For example, `"aws_cloudwatch"` is correct, however `"aws cloud watch"` is incorrect.

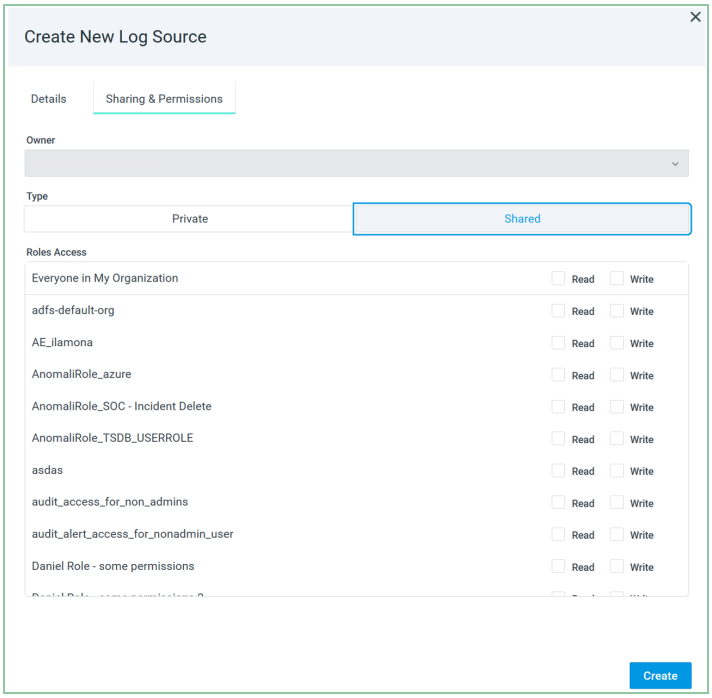
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 4: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 5: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 6: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

AWS Config Notification

Anomali supports the ingestion of AWS Config Notification logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

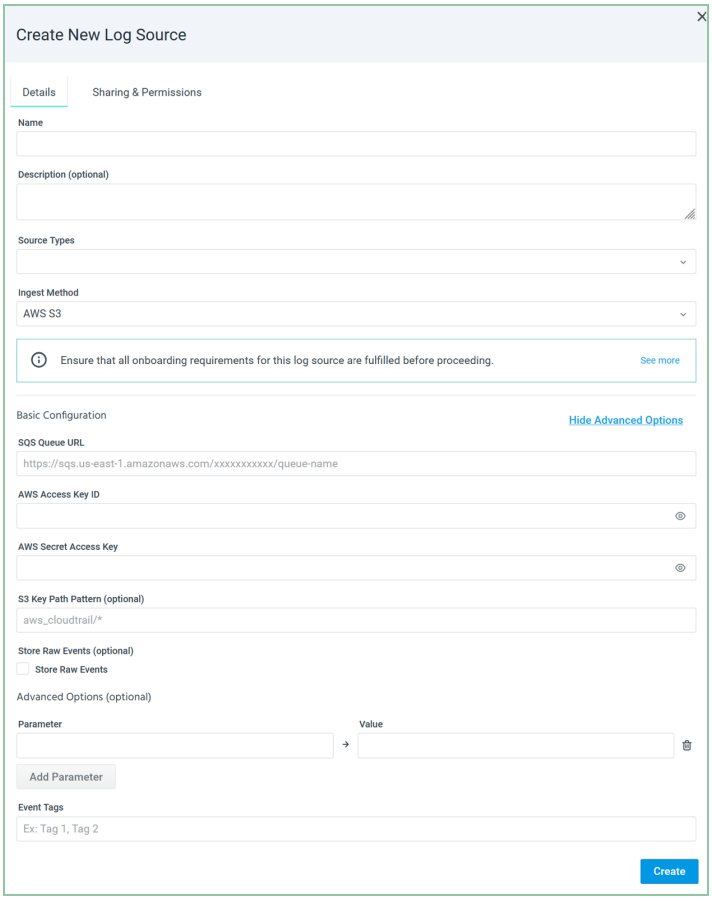
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add AWS Config Notification as new log source



On the Anomali platform, add AWS Config Notification as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `aws_config_notification/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"aws_config_notification"` is correct, however `"AWS Config Notification"` is incorrect.

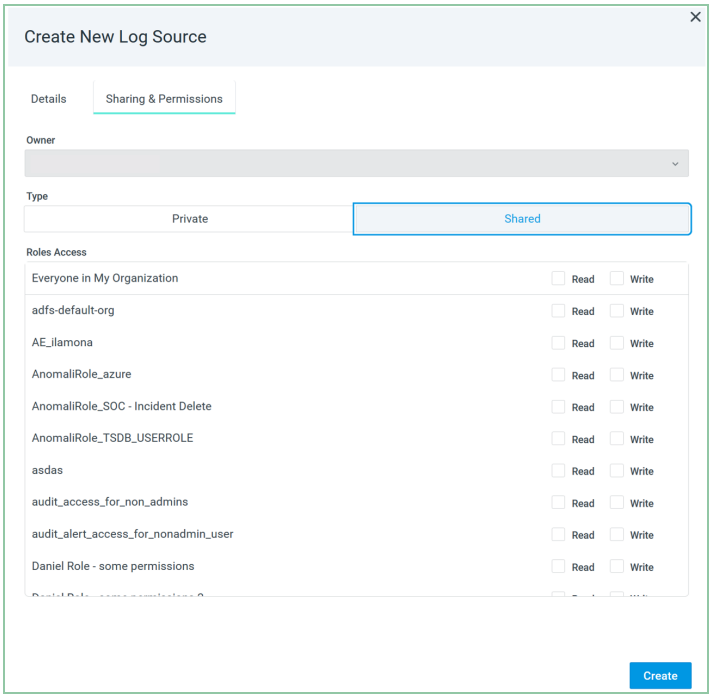
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

AWS EC2

Anomali supports the ingestion of AWS EC2 logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

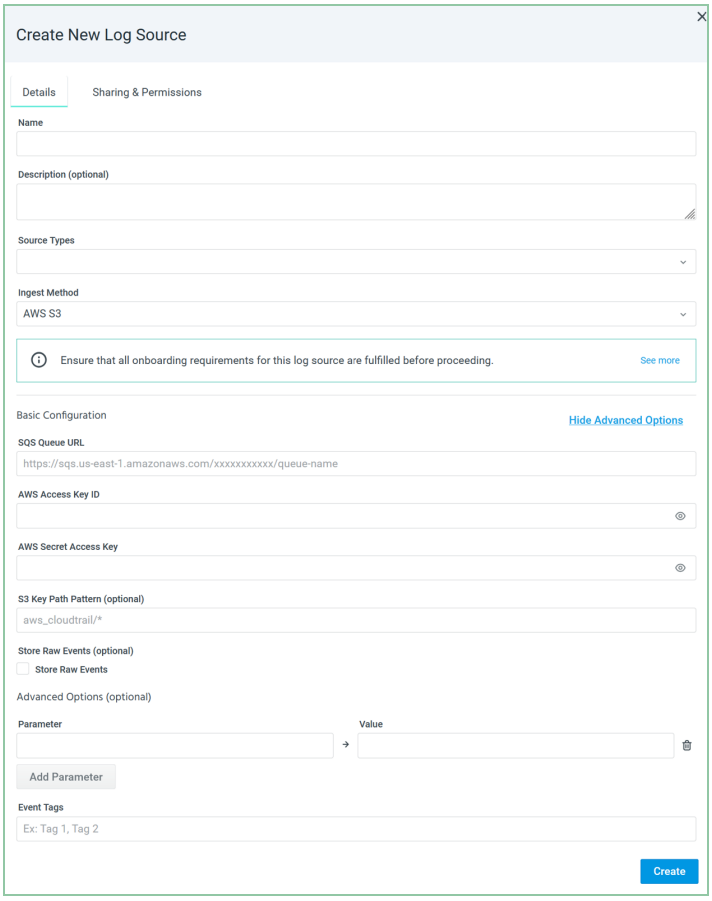
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add AWS EC2 as new log source



On the Anomali platform, add AWS EC2 as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `aws_ec2/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"aws_ec2"` is correct, however `"aws ec2"` is incorrect.

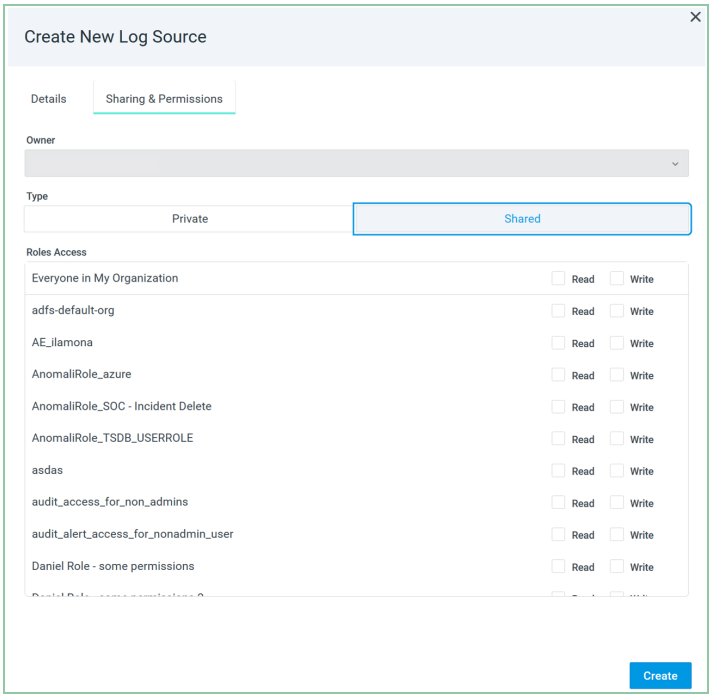
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

AWS GuardDuty

Anomali supports the ingestion of Amazon Web Services (AWS) GuardDuty logs stored in your AWS S3, using Amazon Simple Queue Service (SQS) for notifications.

Once S3 event notifications are configured to send updates to the SQS queue you designate, Anomali automatically pulls the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

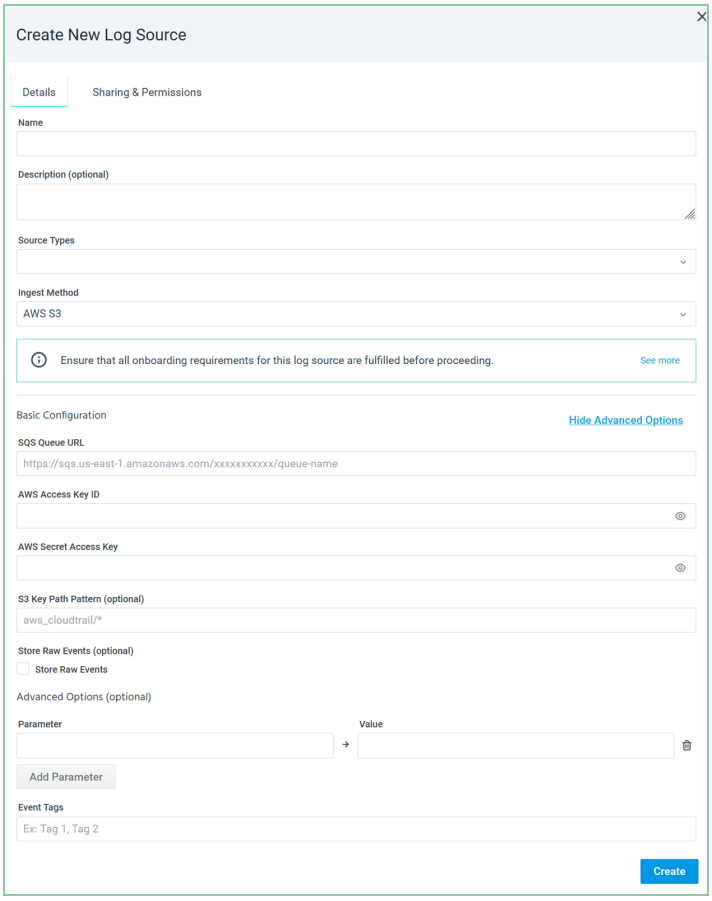
Step 1: Set up SQS queue

To send GuardDuty logs to Anomali, you will first need to set up an Amazon SQS queue.

Step 2: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 3: Add GuardDuty as new log source



On the Anomali platform, add GuardDuty as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `aws_guardduty/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"aws_guardduty"` is correct, however `"aws guard duty"` is incorrect.

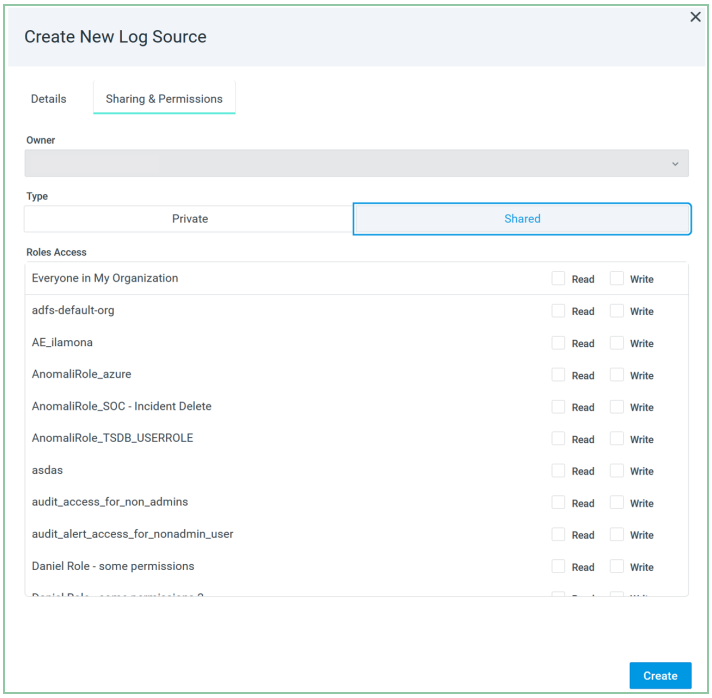
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 4: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 5: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 6: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

AWS Health

Anomali supports the ingestion of AWS Health logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

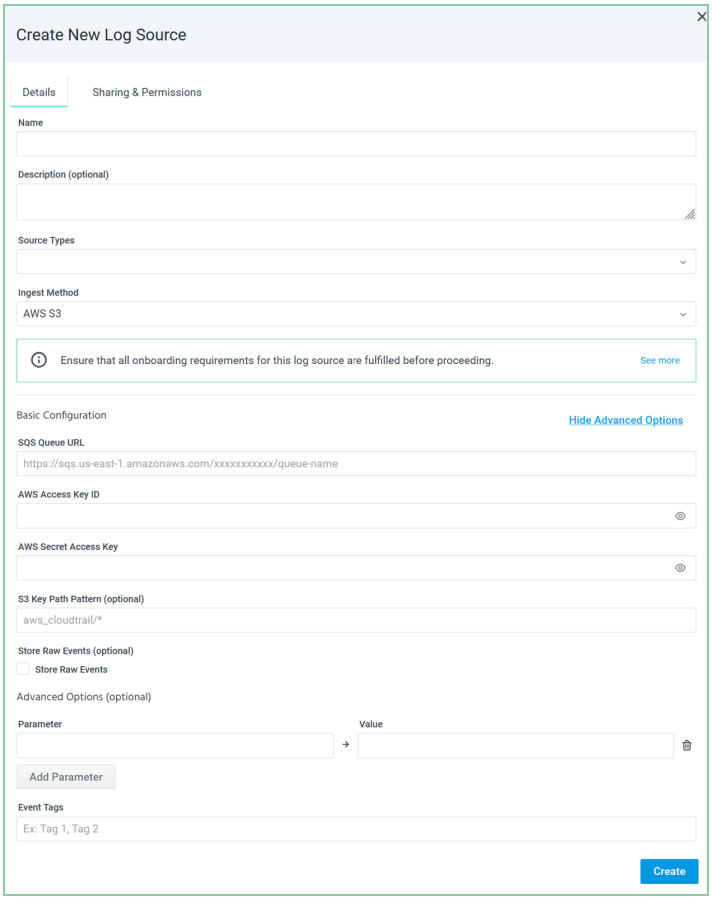
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add AWS Health as new log source



On the Anomali platform, add AWS Health as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `aws_health/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"aws_health"` is correct, however `"aws health"` is incorrect.

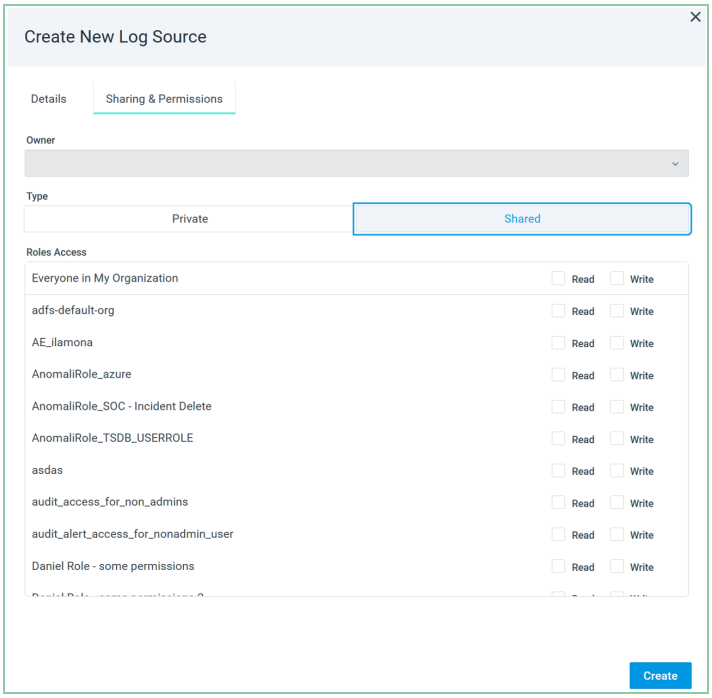
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

AWS SSM

Anomali supports the ingestion of AWS SSM logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

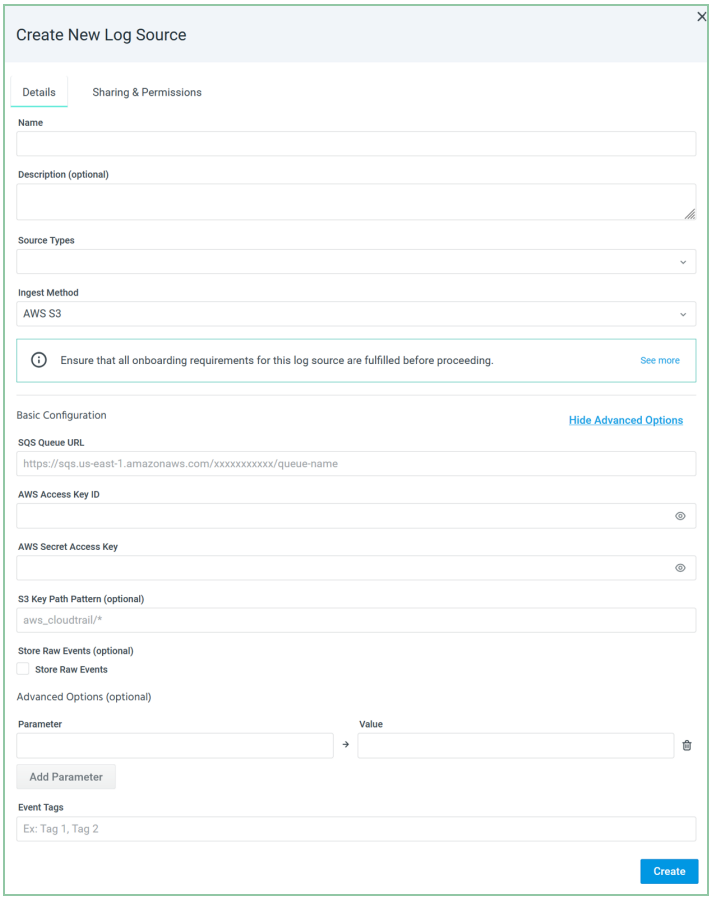
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add AWS SSM as new log source



On the Anomali platform, add AWS SSM as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `aws_ssm/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"aws_ssm"` is correct, however `"aws ssm"` is incorrect.

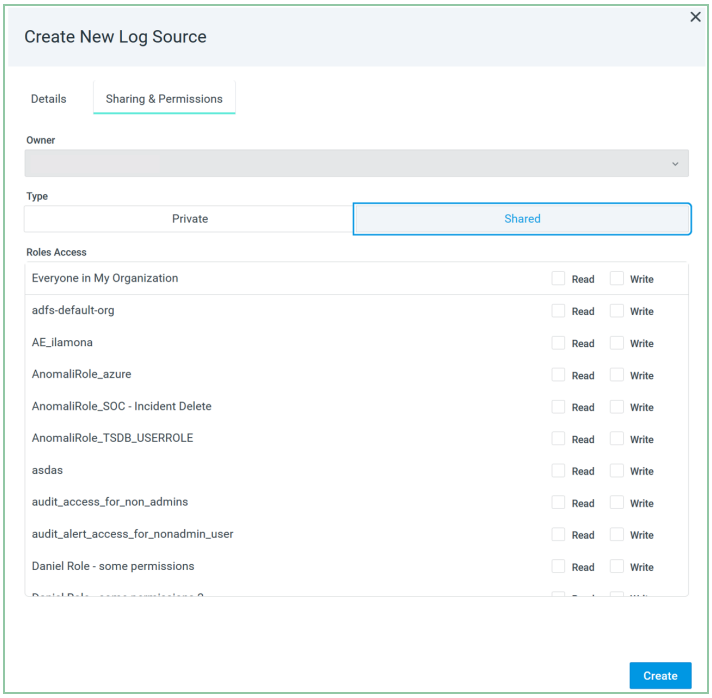
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

AWS VPC DNS

Anomali supports the ingestion of AWS VPC DNS logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

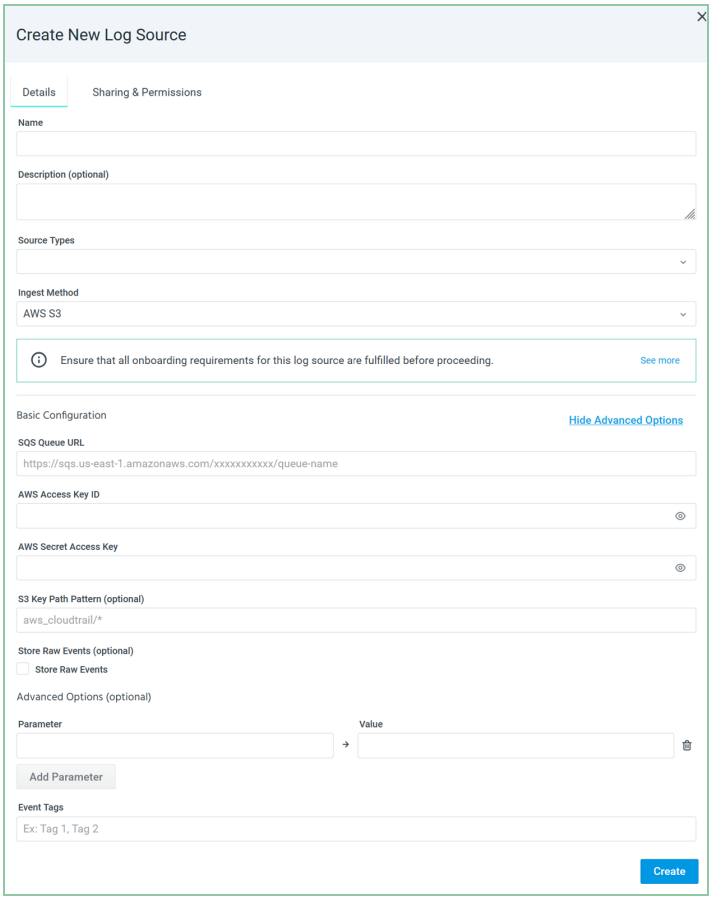
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add AWS VPC DNS as new log source



On the Anomali platform, add AWS VPC DNS as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `aws_vpc_dns/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"aws_vpc_dns"` is correct, however `"aws vpc dns"` is incorrect.

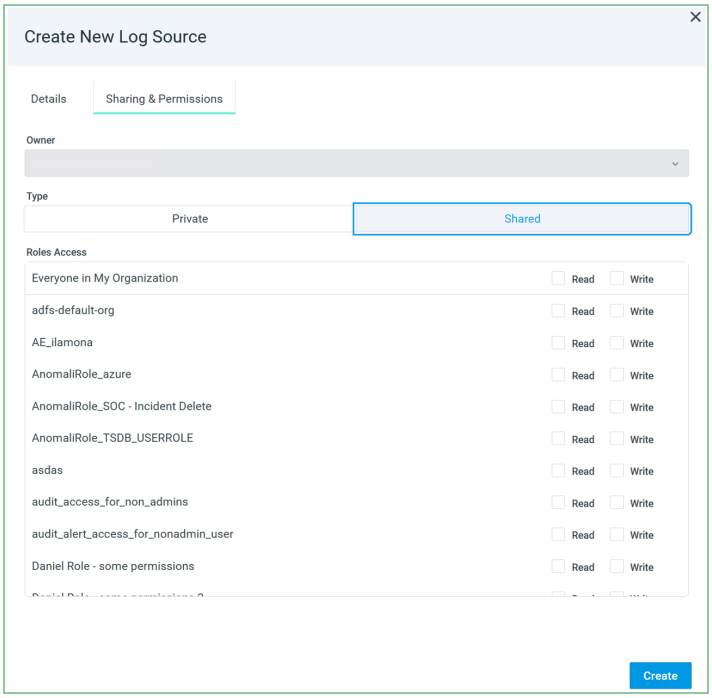
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

AWS VPC Flow

Anomali supports the ingestion of Amazon Web Services (AWS) VPC Flow logs stored in your AWS S3, using Amazon Simple Queue Service (SQS) for notifications.

Once S3 event notifications are configured to send updates to the SQS queue you designate, Anomali automatically pulls the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

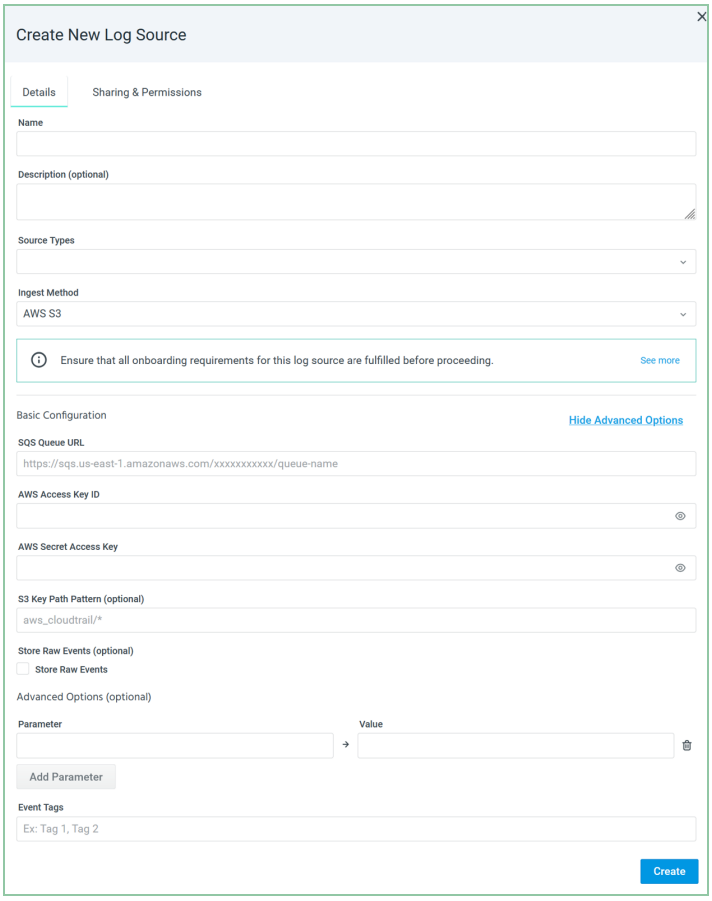
Step 1: Set up SQS queue

To send VPC logs to Anomali, you will first need to set up an Amazon SQS queue.

Step 2: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 3: Add VPC as new log source



On the Anomali platform, add VPC as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `aws_vpcflow/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"aws_vpcflow"` is correct, however `"aws vpc flow"` is incorrect.

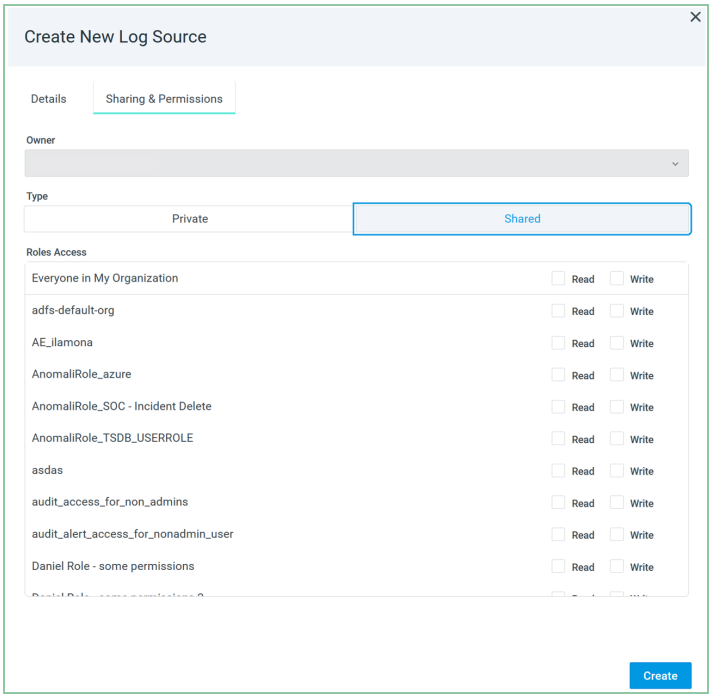
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 4: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 5: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 6: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

AWS WAF

Anomali supports the ingestion of Amazon Web Services (AWS) WAF logs stored in your AWS S3, using Amazon Simple Queue Service (SQS) for notifications.

Once S3 event notifications are configured to send updates to the SQS queue you designate, Anomali automatically pulls the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

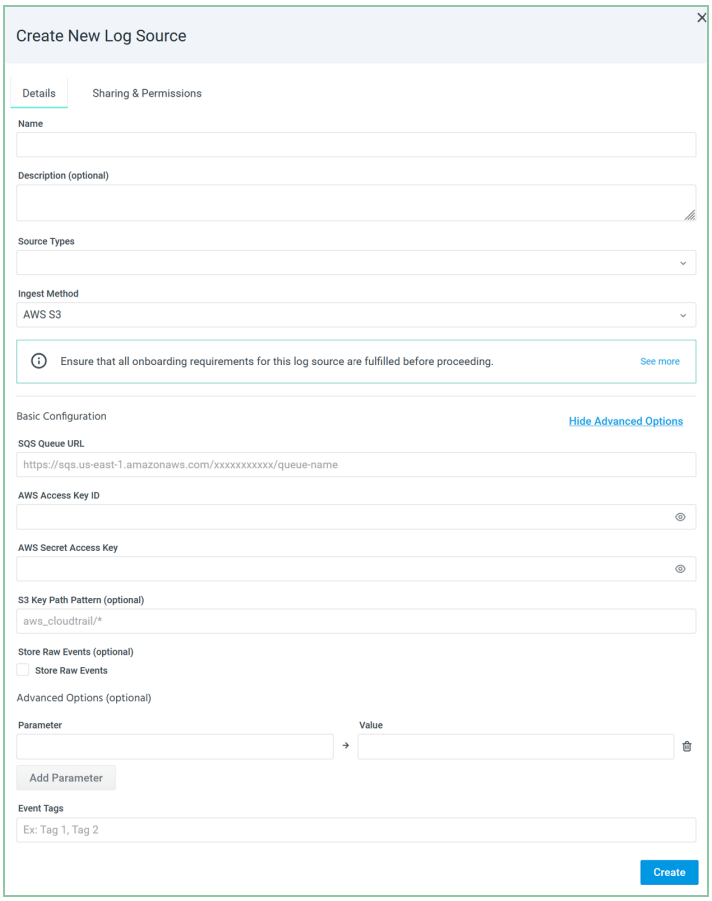
Step 1: Set up SQS queue

To send WAF logs to Anomali, you will first need to set up an Amazon SQS queue.

Step 2: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 3: Add WAF as new log source



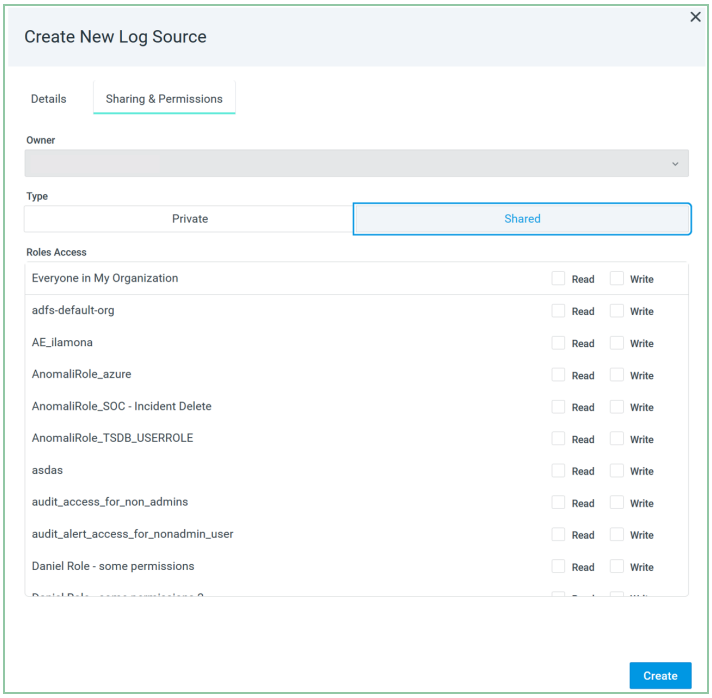
On the Anomali platform, add WAF as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:
   a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.
   b. **AWS Secret Access Key**: Provide the AWS secret access key.
   c. **AWS Access Key ID**: Enter the AWS Access ID.
   d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:
      - Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `aws_waf/year=2025/month=03/day=22/events/event_data_logs/`.
      - Sourcetype name must not contain any spaces: For example, `"aws_waf"` is correct, however `"aws waf"` is incorrect.
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:
   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 4: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.

2. Type: Select the type of permission assigned to the view:

   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.

   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 5: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 6: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Microsoft Azure Active Directory

Anomali supports the ingestion of Microsoft Azure Active Directory (AD) logs either through "Azure Storage account" below or "AWS S3" on page 495.

Azure Storage account

Prerequisites

1. Your organization must have an active subscription to Azure.
2. Your organization must have a Microsoft 365 E5 license. Refer to the Microsoft website for details.
3. You must deploy Microsoft Endpoint Defender to the hosts you intend to manage. See Microsoft's guide to Onboard devices and configure Microsoft Defender for Endpoint capabilities for details.

Step 1: Set Up Azure Resources

Complete Microsoft Azure workflows for the following activities to set up your Azure environment.

1. Create an Azure function based on the Azure Event Grid trigger template. See Microsoft's guide to Create Azure Function for details.

   Under **Code + Test**, paste the following `event_sender.js` code provided by Anomali for this integration. Replace `<username>:<apikey>` with the username and API key for the ThreatStream user account you have provisioned to be a service account for this integration (refer to "Prerequisites" above).

```
const https = require('https');
module.exports = async function (context, eventGridEvent) {

        const eventData = JSON.stringify(eventGridEvent);

                const options = {
                hostname: 'api.threatstream.com',
                port: 443,
                path: '/api/v1/xdr/cloud_logsource/azure_storage/event/',
                method: 'POST',
                headers: {
                        'Content-Type': 'application/json',
                        'Content-Length': eventData.length,
```

```
                        'Authorization': 'apikey <username>:<apikey>'
                }
        };

        const req = https.request(options, (res) => {
                console.log('statusCode:', res.statusCode);
                console.log('headers:', res.headers);

        res.on('data', (d) => {
                process.stdout.write(d);
                });
        });

        req.on('error', (e) => {
                console.error(e);
        });

        req.write(eventData);
        req.end();
};
```

2. Provision an Azure Storage account for this integration.

   a. Create an Azure Storage account. See Microsoft's guide to Create a storage account for more details.

   b. After the Storage account has been created, add an Event Subscription to the Storage account configuration:

      i. Go to **Events** and click **+ Event Subscription**.

      ii. Select **Event Grid Schema**.

      iii. Under Filter to Event Types, select **Blob Created**.

      iv. Under Endpoint Type, select **Azure Function**.

      v. For Endpoint, select the Azure function created for this integration in the previous step. See Microsoft's guide to Subscribe to custom topic for details.

   c. Copy the Storage account name and Storage account access key to a safe

place that you can access when you complete the Security Analytics log source configuration.

See Microsoft's guide on how to View account access keys for more details.

Step 2: Configure Endpoints to Stream Events to Azure Storage

Enable the Microsoft Defender Streaming API so managed hosts can stream event logs to Azure Storage.

1. Log in to Microsoft 365 Defender as a global admin or security admin.
2. Go to **Settings** > **Microsoft 365 Defender** > **Streaming API**.
3. Click **Add**.
4. In the Add new Streaming API settings, specify the Azure Storage account information set up in "Step 1: Set Up Azure Resources" on page 491.
5. Select only the following events: **AlertEvidence**, **AlertInfo**, **DeviceNetworkEvents**, **DeviceProcessEvents**, **DeviceFileEvents**, **DeviceLogonEvents**, **DeviceFileCertificateInfo**, **DeviceImageLoadEvents**, **EmailEvents**, **EmailAttachmentInfo**, **EmailUrlInfo**.

After you have deployed the required Microsoft components, Windows Defender will start capturing the events from the on-boarded devices.

Step 3: Add Azure Active Directory as new log source

To add Defender as a new log source on the Anomali platform:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select **Azure Active Directory** as the source type.
6. Select **API** as the ingestion method.
7. Select API as the ingest method.
8. Provide the Basic Configuration details:

a. **Azure Storage Account Name**: Type the provisioned storage account name from "Step 1: Set Up Azure Resources" on page 491.

b. **Azure Storage Account Access Key**: Paste the key for the provisioned account from "Step 1: Set Up Azure Resources" on page 491.

c. **Wildcard Log Schema**: Provide the wildcard log schema.

d. (Optional) **Raw events**: Select **Enable** to collect and store the entire event log that is available from the log source.

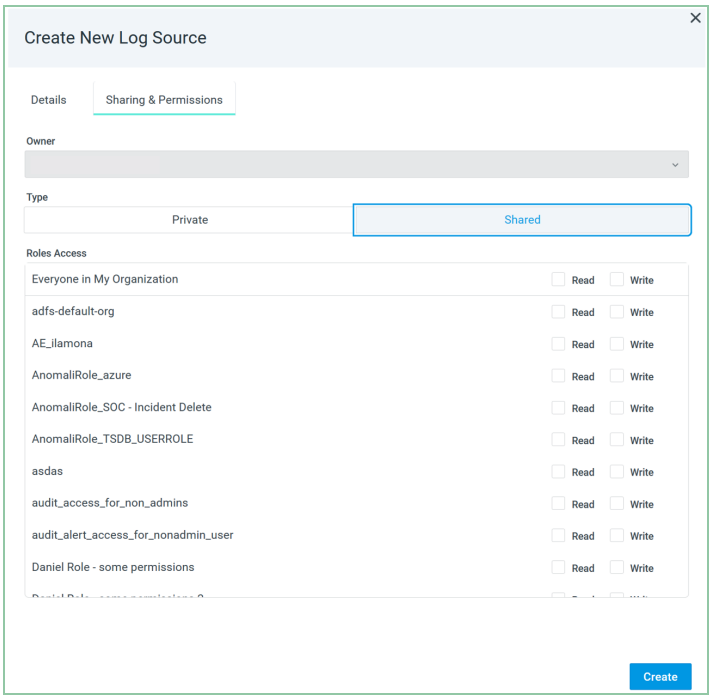
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 4: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 5: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 6: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

AWS S3

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

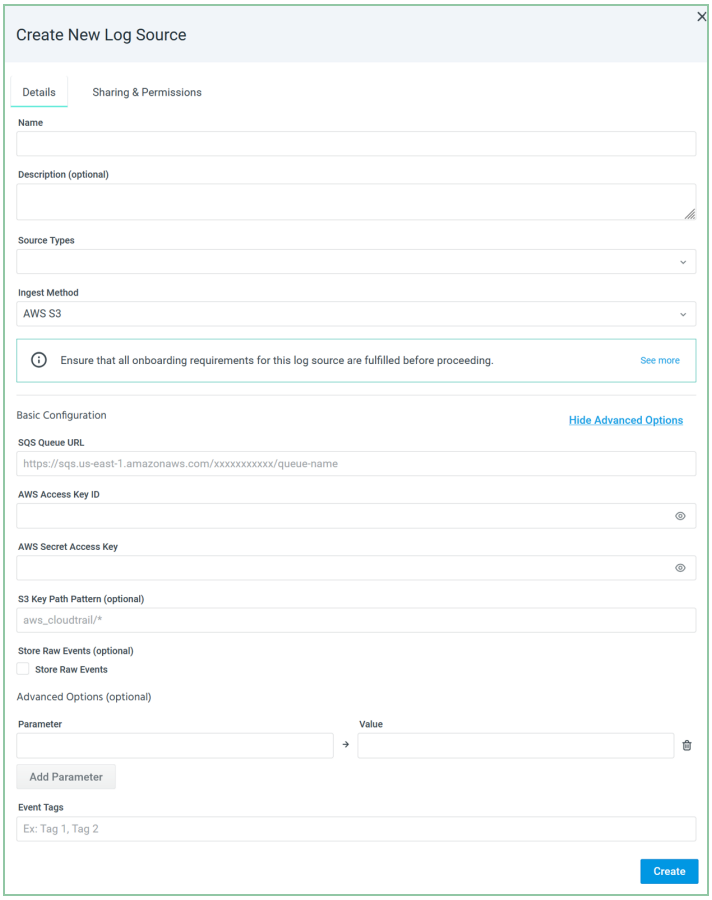
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Azure Active Directory as new log source

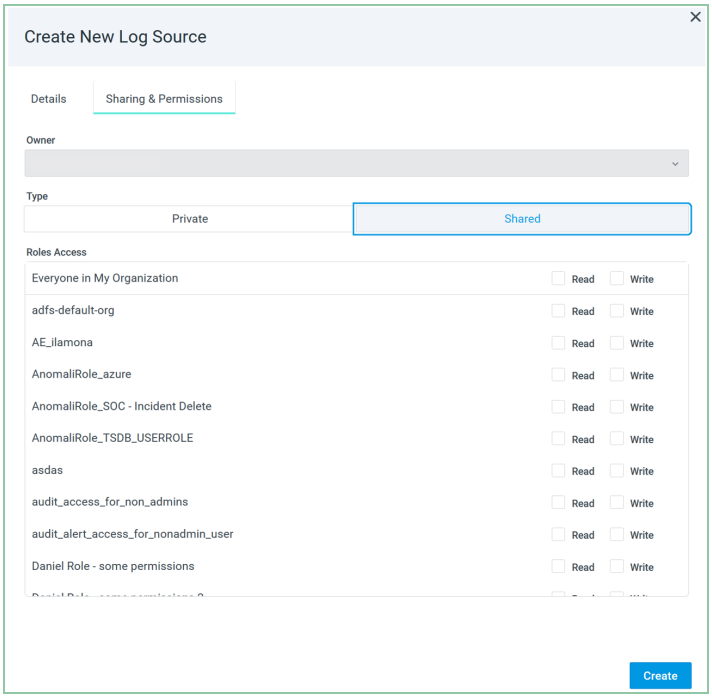


On the Anomali platform, add Azure Active Directory as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.

6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:
   a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.
   b. **AWS Secret Access Key**: Provide the AWS secret access key.
   c. **AWS Access Key ID**: Enter the AWS Access ID.
   d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:
      - Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `azure_active_directory/year=2025/month=03/day=22/events/event_data_logs/`.
      - Sourcetype name must not contain any spaces: For example, `"azure_active_directory"` is correct, however `"azure_active_directory"` is incorrect.
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:
   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.
   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.
10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Microsoft Azure Sentinel

Anomali Security Analytics can ingest event log data from Microsoft Azure Sentinel. The following article explains the steps you must complete to ingest Azure Sentinel logs into Anomali.

Onboarding steps

Step 1: Register with Azure Sentinel to Access the Log Analytics Workspace

Create a dedicated Microsoft Entra ID app for the integration. Refer to Microsoft documentation for complete details.

To create the app and configure necessary permissions:

1. On the Azure portal, go to **Microsoft Entra ID > App Registrations**.
2. Click **New Registration**.
3. Register an application:
   a. Specify a user-facing display name. For example, `Azure Sentinel Integration with Anomali`.
   b. Select **Accounts in this organizational directory** as the account type.
   c. Leave **Redirect URI** blank.
   d. Click **Register**.
4. Once the app is registered, select it to display its details.
5. Copy the Application (client) ID and Directory (tenant) ID. You will need these IDs later.

Step 2: Configure API permissions

1. Configure API permissions:
   a. In the left menu, go to **API permissions** and click **Add a permission**.
   b. Search for and select `Log Analytics API`.
   c. Select **Application permissions**, select the **Data.Read** check box, and click **Add permissions.**

d. In the Configured permissions table, click **Grant admin consent** for your organization and click **Yes** in the dialog box.

Step 3: Set Client Secret

1. Set up a client secret for the app.

   a. In the left menu, go to **Certificates and secrets** and click **New client secret**.

   b. Specify a description, select an expiration, and click **Add**. The secret is added to the Client secrets table.

   c. Copy the client secret to a secure location. You will need to provide it to Anomali later.

Step 4: Grant permissions

1. Grant the application you registered earlier (`Azure Sentinel Integration with Anomali`) access to the Log Analytics workspace that contains the Sentinel logs on Azure:

   a. Go to the Log Analytics workspace that contains the Sentinel logs. In our example, it is `staging-security-ws`.

   b. Copy the Workspace ID. You will need to provide this ID to Anomali later.

   c. Click **Access Control (IAM) > Add > Add role assignment**.

      i. Select **Log Analytics Reader** from the Role list.

      ii. Enter the name of your application in the **Assign access to** > **Select** field. Once the name is visible in the list, select it.

      iii. Click **Save**.

Step 5: Add Azure Sentinel as new log source

To add Azure Sentinel as a new log source on the Anomali platform:

1. Navigate to **Search** > **Log Source Management**.

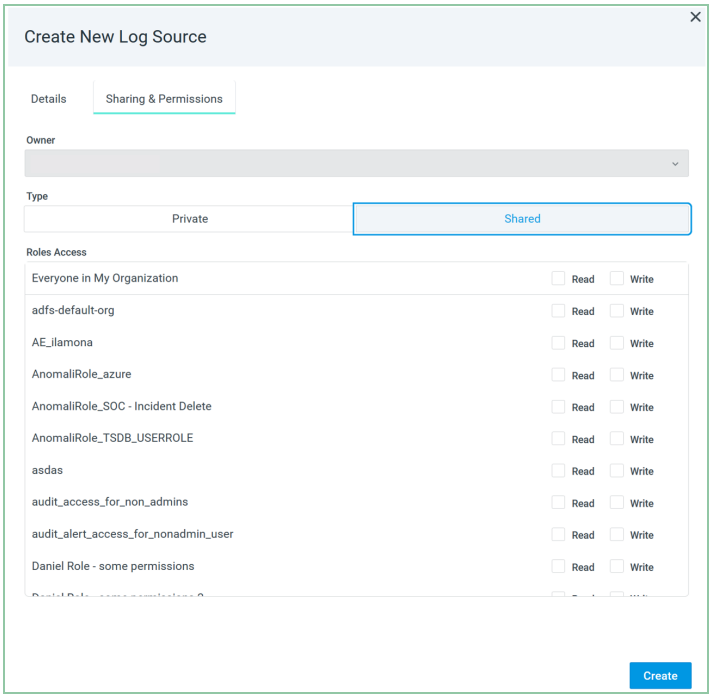
2. Click **New** to add a new log source.

3. Enter a name for the log source.

4. (Optional) Enter a description for the log source.

5. Select **Azure Sentinel** as the source type.
6. Select **API** as the ingestion method.
7. Select API as the ingest method.
8. Provide the Basic Configuration details:
    a. **Client Secret** App client secret associated with the Application ID above.
    b. (Optional) **Azure Sentinel Queries**: Provide the Azure Sentinel queries.
    c. (Optional) **Azure Sentinel Tenant ID**: Enter the tenant ID assigned to your organization.
    d. (Optional) **Azure Sentinel Client ID**: Enter the application ID of the Azure AD app that can access your Log Analytics workspace.
    e. (Optional) **Azure Sentinel Workspace ID**: Enter the Workspace ID of the Log Analytics workspace.
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:
    a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.
    b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.
10. Click **Save** to add the log source.

Step 6: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 7: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 8: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Bomgar

Anomali supports the ingestion of Bomgar logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

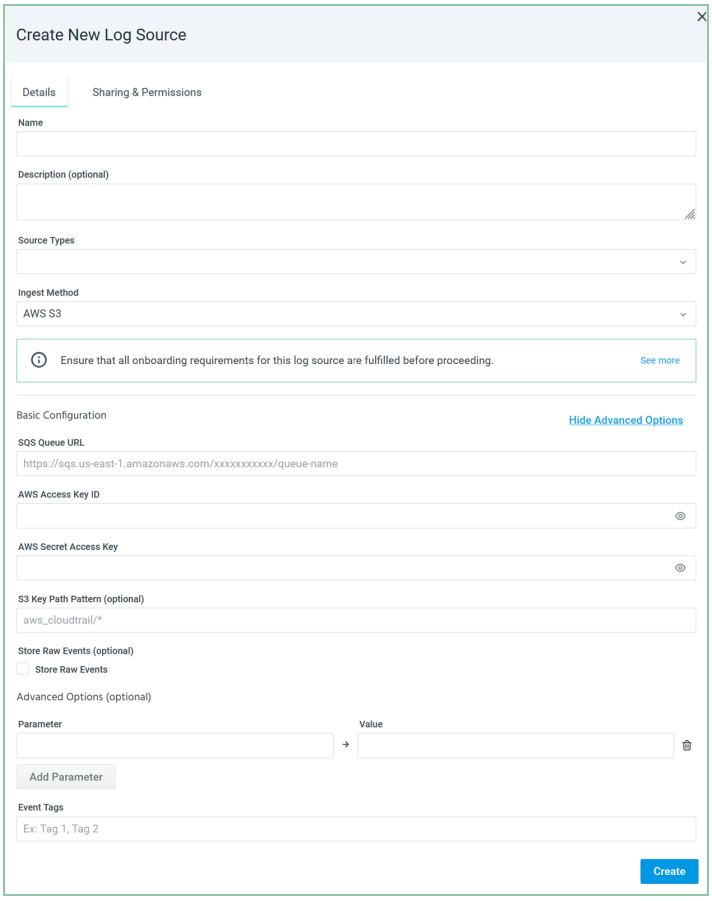
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Bomgar as new log source



On the Anomali platform, add Bomgar as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `bomgar/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"bomgar"` or `"bomgar_sourcetype"` are correct, however `"bomgar sourcetype"` is incorrect.

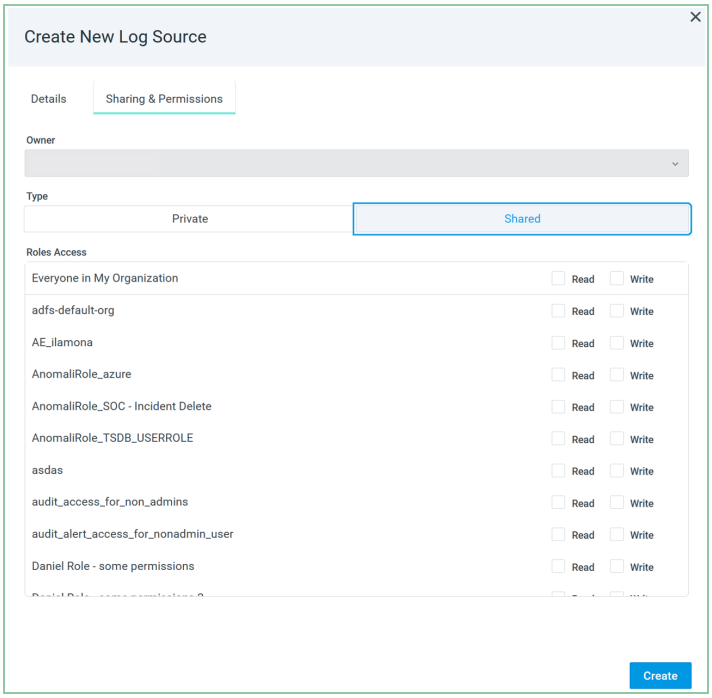
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Carbon Black

Anomali supports the ingestion of Carbon Black logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

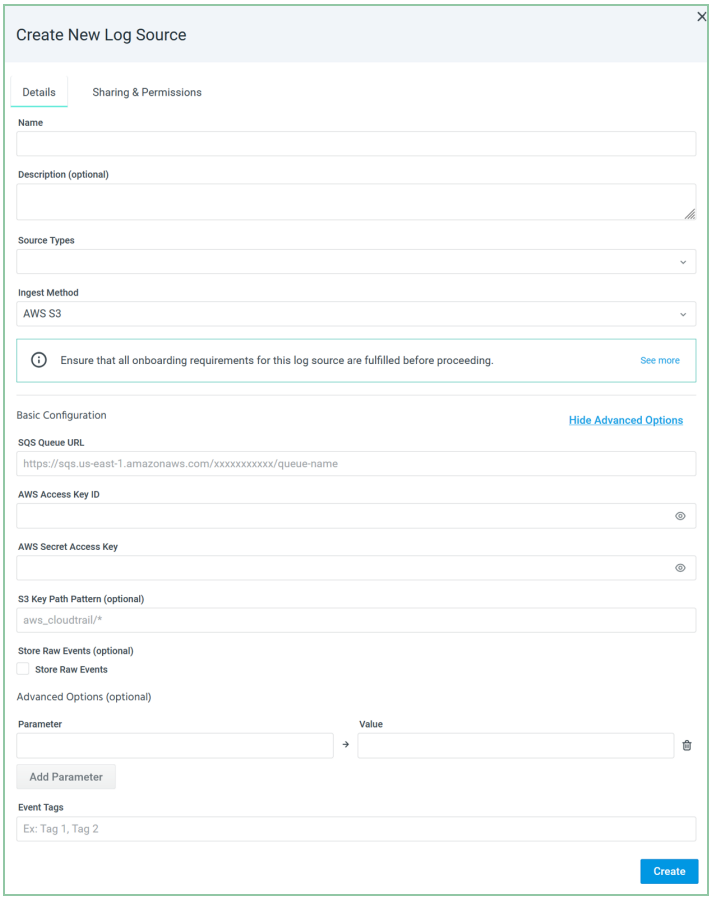
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Carbon Black as new log source



On the Anomali platform, add Carbon Black as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `carbon_black/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"carbon_black"` is correct, however `"carbon black"` is incorrect.

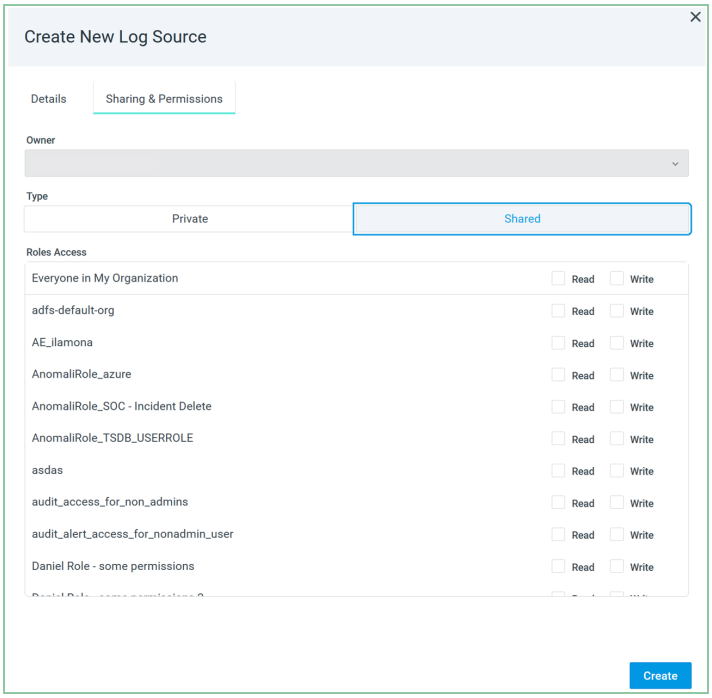
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Catalina

Anomali supports the ingestion of Catalina logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

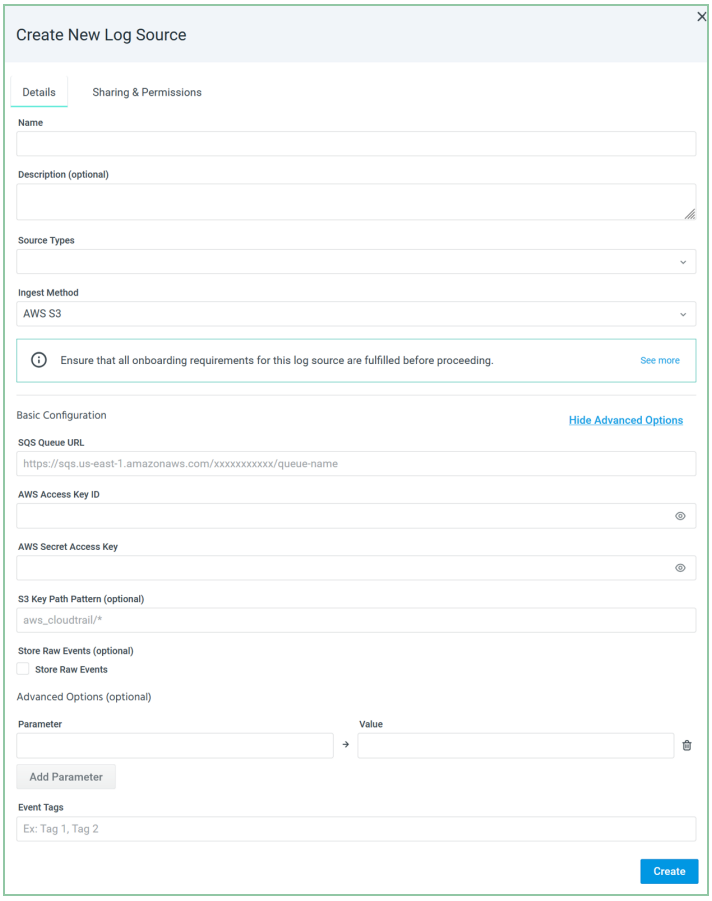
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Catalina as new log source



On the Anomali platform, add Catalina as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `catalina/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"catalina"` or `"catalina_sourcetype"` are correct, however `"Catalina sourcetype"` is incorrect.

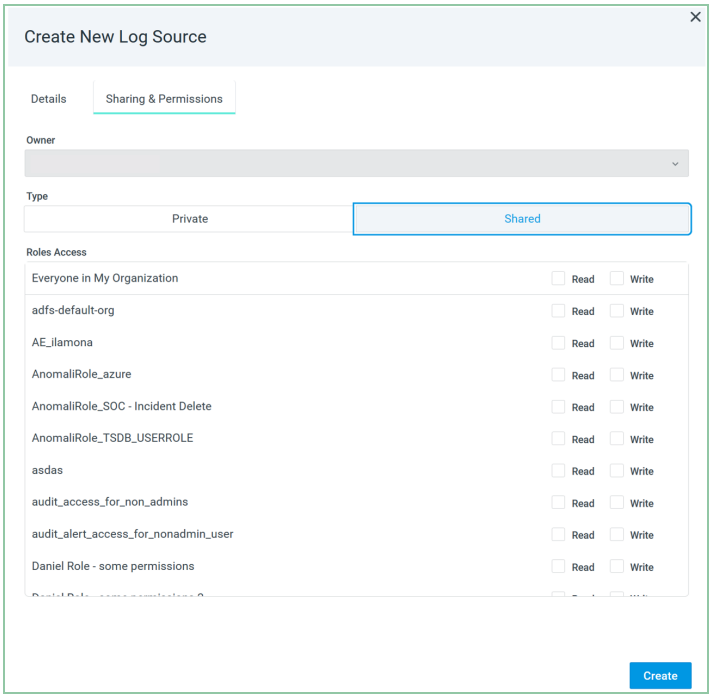
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Cisco ACS

Anomali supports the ingestion of Cisco ACS logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

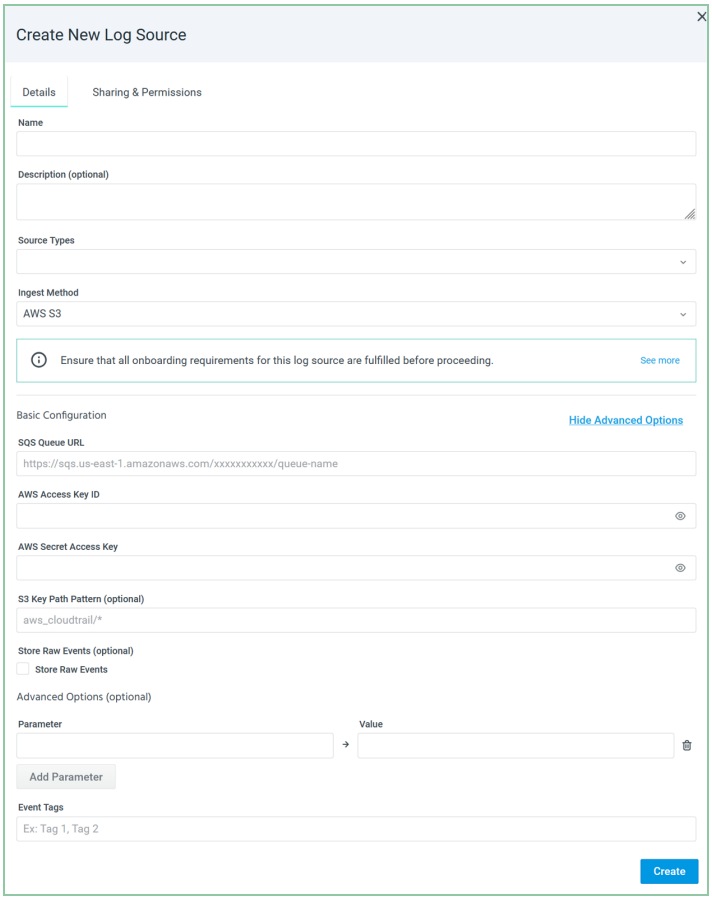
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Cisco ACS as new log source



On the Anomali platform, add Cisco ACS as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `cisco_acs/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"cisco_acs"` is correct, however `"Cisco ACS"` is incorrect.

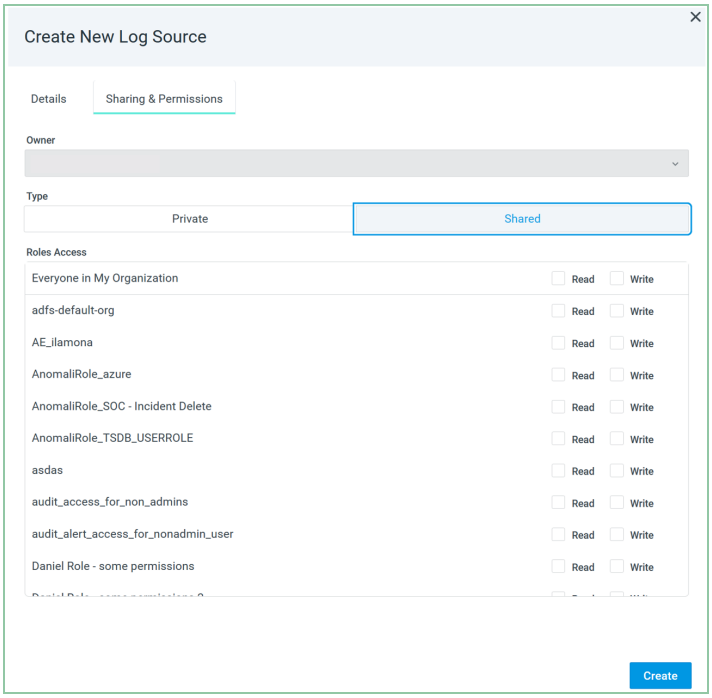
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Cisco ASA

Anomali supports the ingestion of Cisco ASA logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

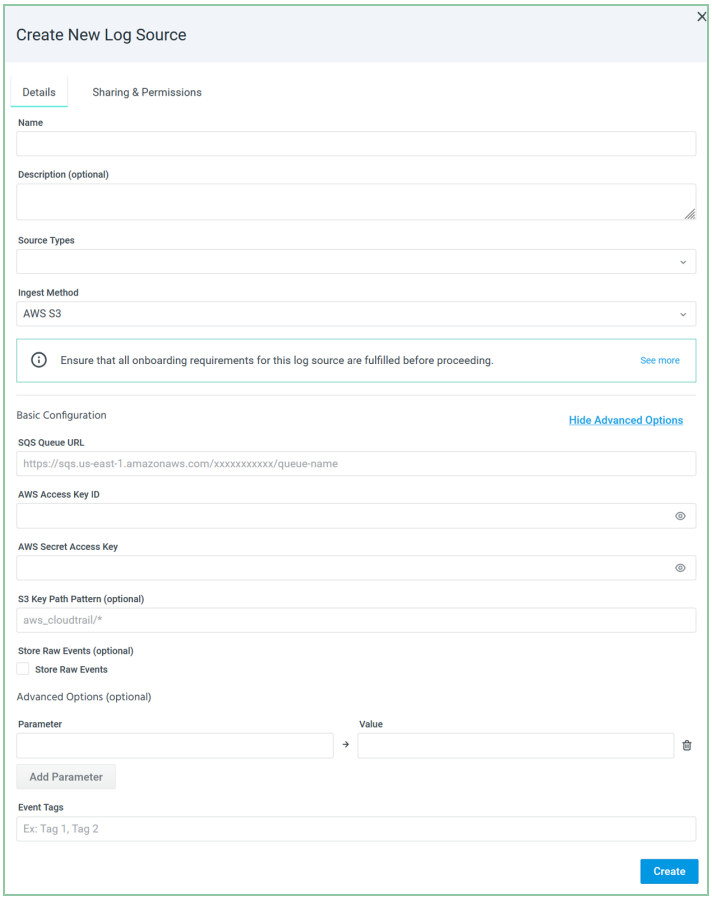
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Cisco ASA as new log source



On the Anomali platform, add Cisco ASA as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `cisco_asa/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"cisco_asa"` is correct, however `"cisco asa"` is incorrect.

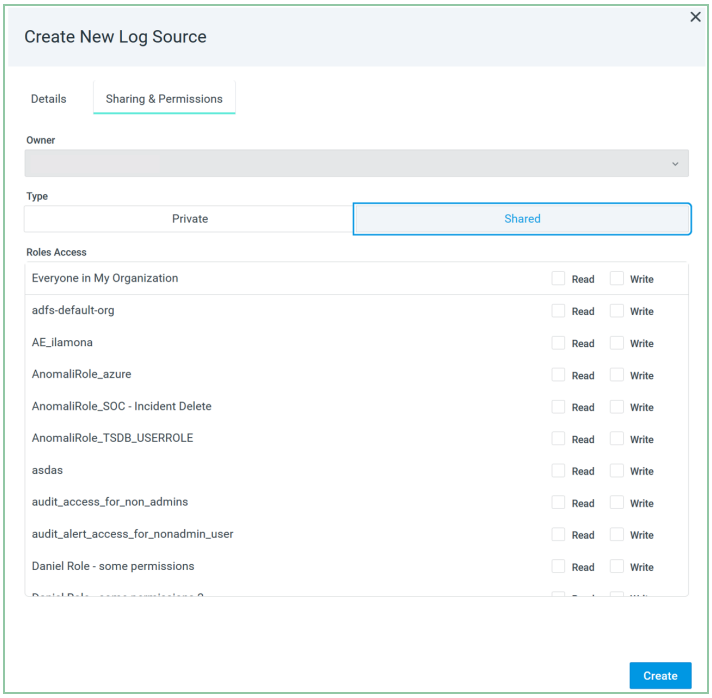
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Cisco ESA

Anomali supports the ingestion of Cisco ESA logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

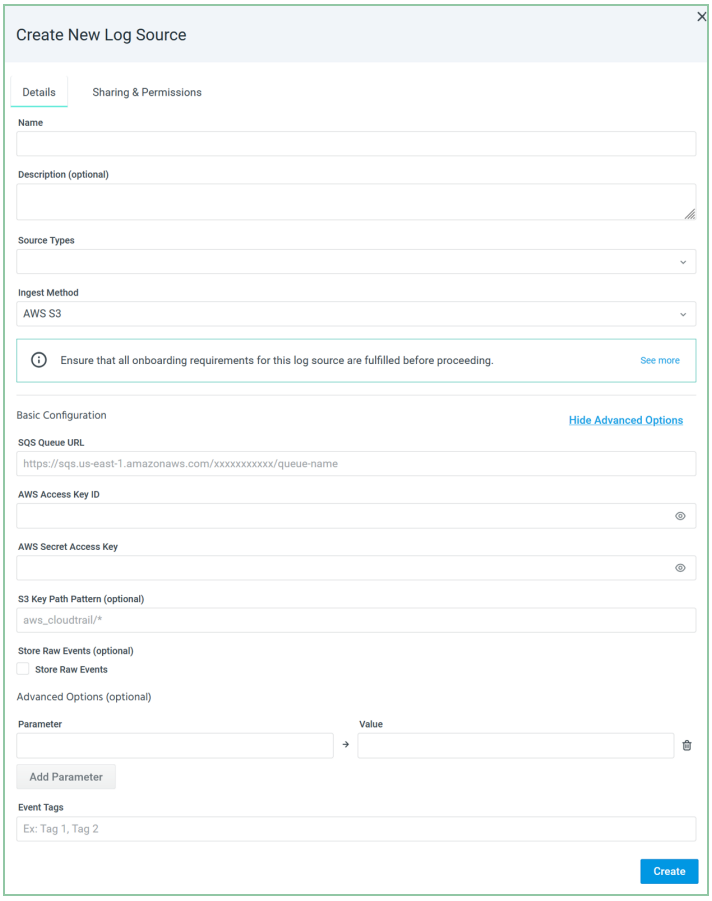
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Cisco ESA as new log source



On the Anomali platform, add Cisco ESA as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `cisco_esa/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"cisco_esa"` is correct, however `"cisco esa"` is incorrect.

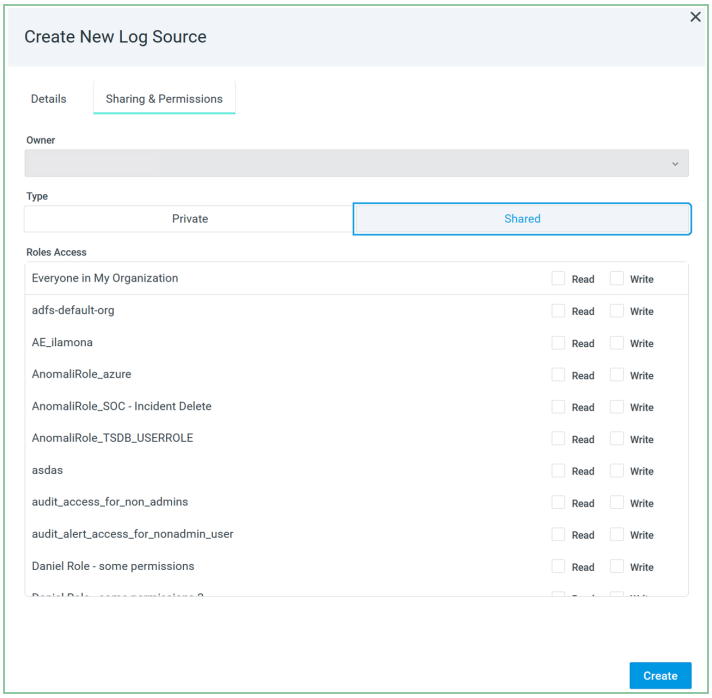
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions

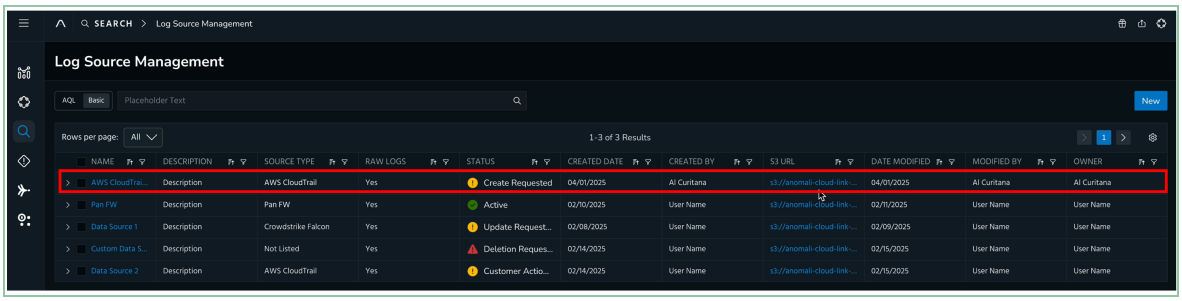


You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.



Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Cisco ESA Amp

Anomali supports the ingestion of Cisco ESA Amp logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

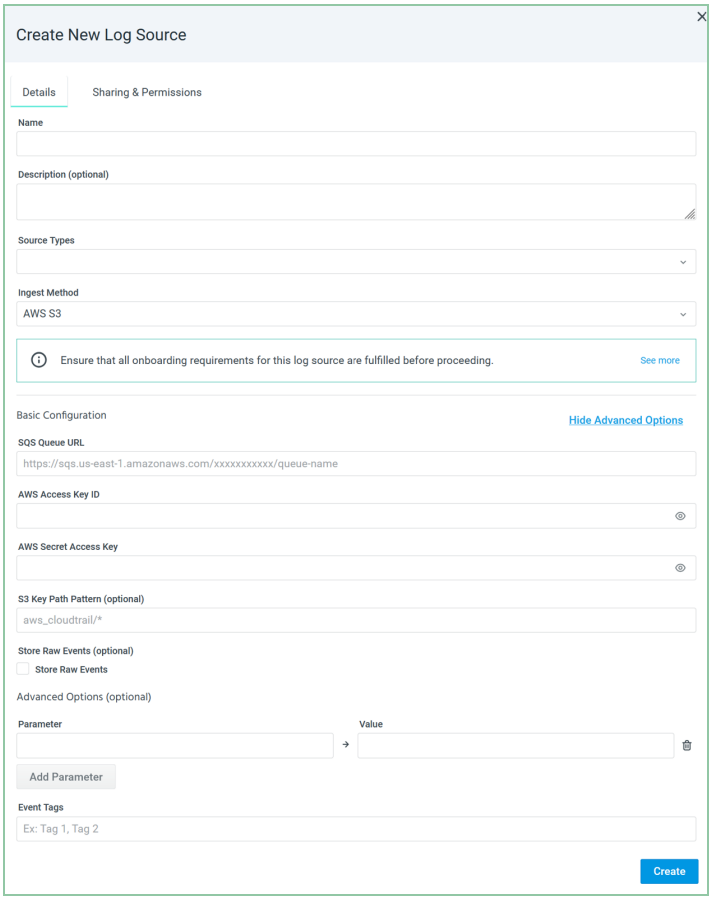
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Cisco ESA Amp as new log source



On the Anomali platform, add Cisco ESA Amp as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `cisco_esa_amp/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"cisco_esa_amp"` is correct, however `"cisco esa amp"` is incorrect.

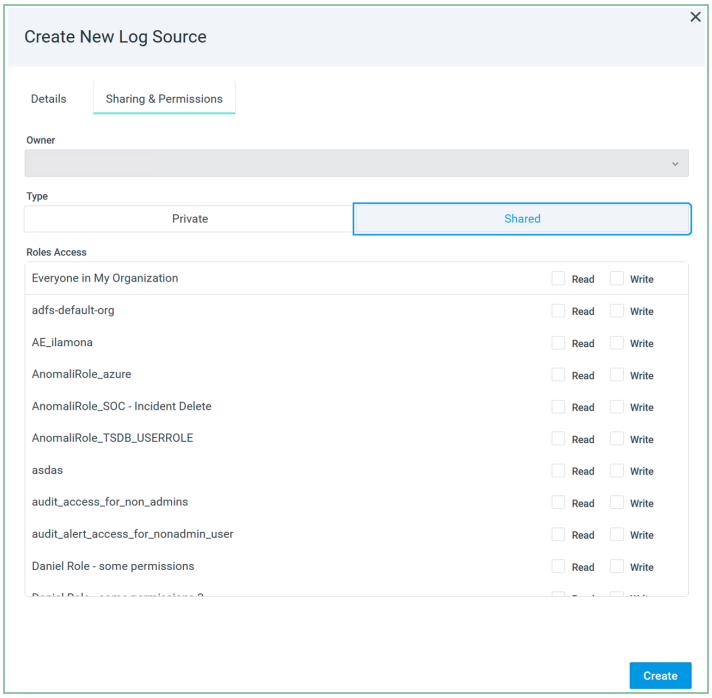
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Cisco ESA AntiSpam

Anomali supports the ingestion of Cisco ESA AntiSpam logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

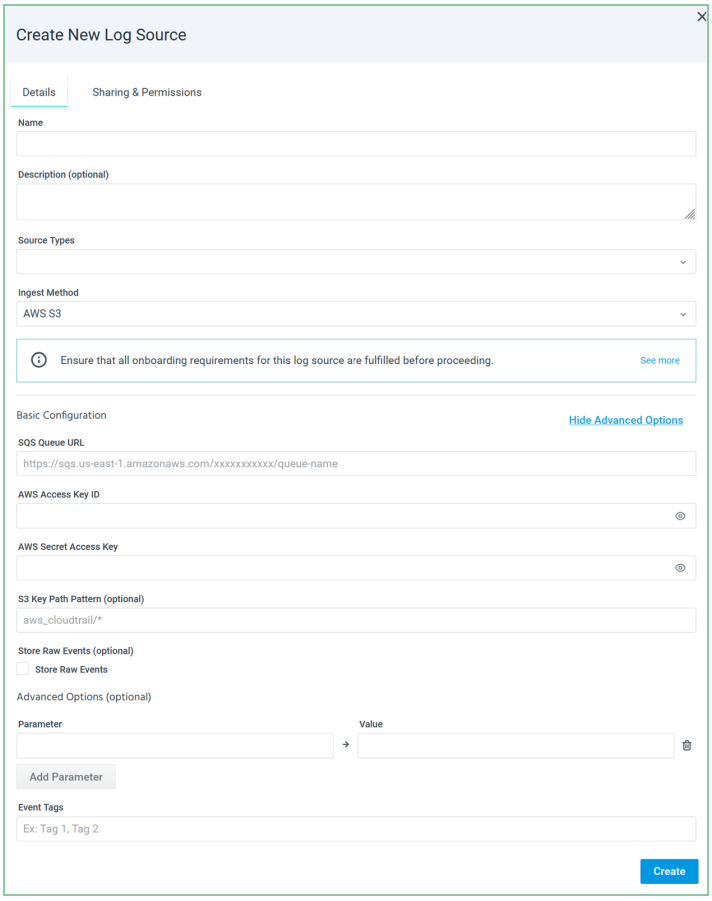
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Cisco ESA AntiSpam as new log source



On the Anomali platform, add Cisco ESA AntiSpam as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `cisco_esa_antispam/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"cisco_esa_antispam"` is correct, however `"cisco esa antispam"` is incorrect.

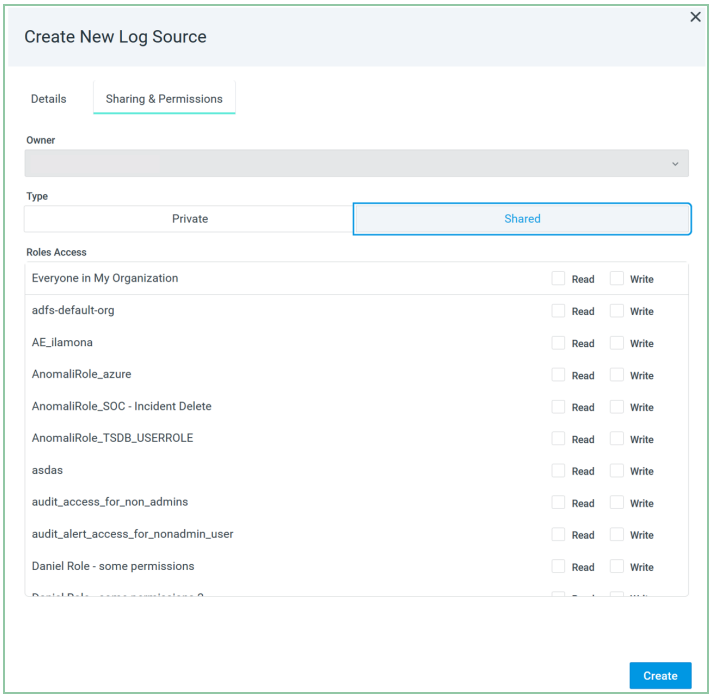
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Cisco ESA Antivirus

Anomali supports the ingestion of Cisco ESA Antivirus logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

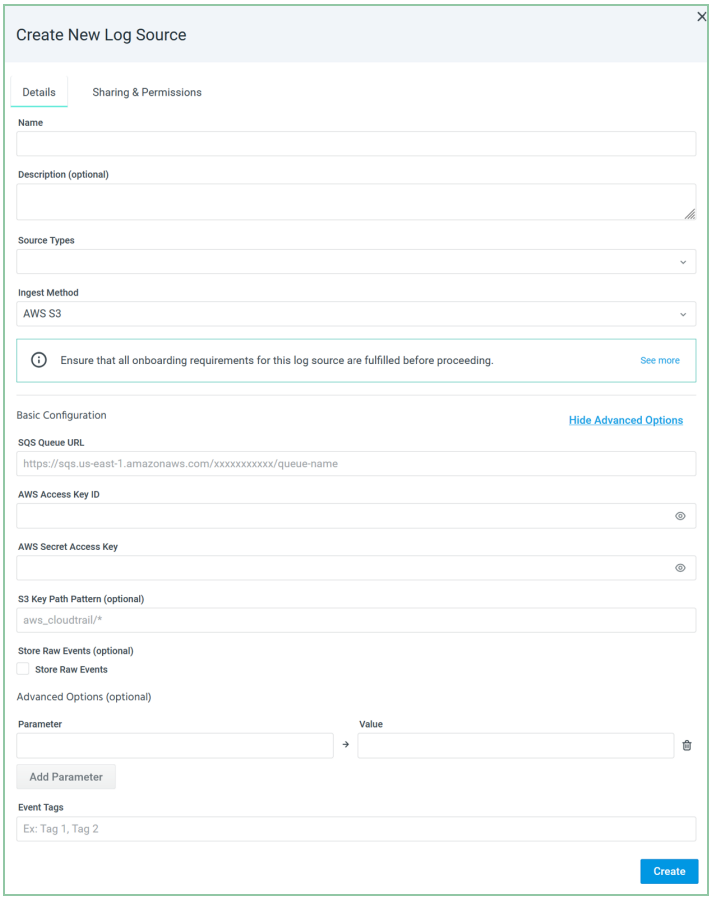
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Cisco ESA Antivirus as new log source



On the Anomali platform, add Cisco ESA Antivirus as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `cisco_esa_antivirus/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"cisco_esa_antivirus"` is correct, however `"cisco esa antivirus"` is incorrect.

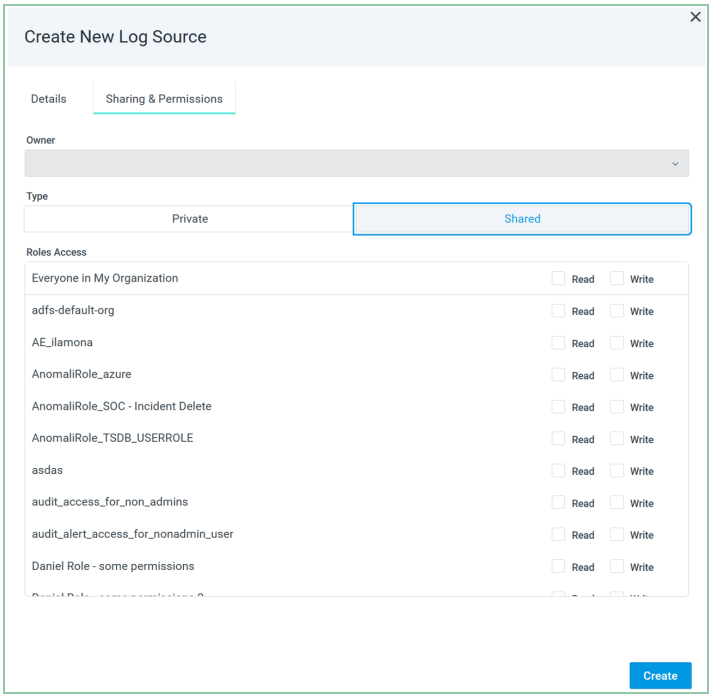
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Cisco ESA Authentication

Anomali supports the ingestion of Cisco ESA Authentication logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

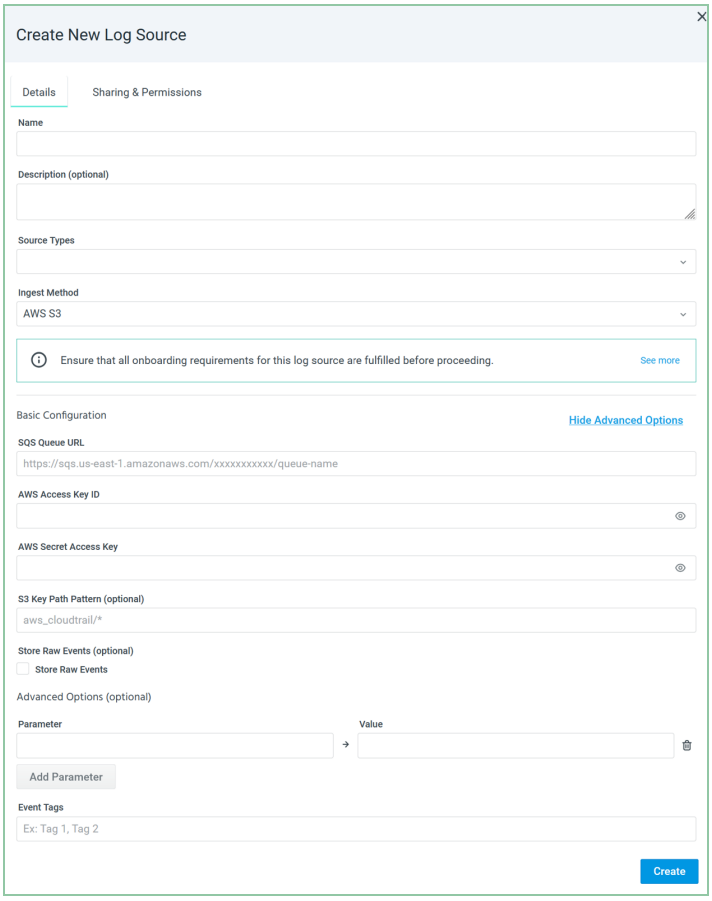
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Cisco ESA Authentication as new log source



On the Anomali platform, add Cisco ESA Authentication as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `cisco_esa_authentication/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"cisco_esa_authentication"` is correct, however `"cisco esa authentication"` is incorrect.

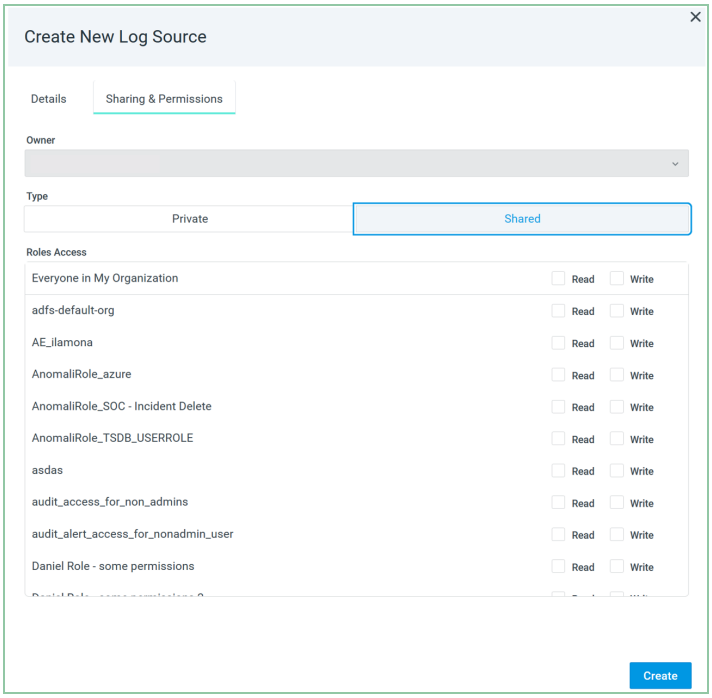
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Cisco ESA Bounce

Anomali supports the ingestion of Cisco ESA Bounce logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

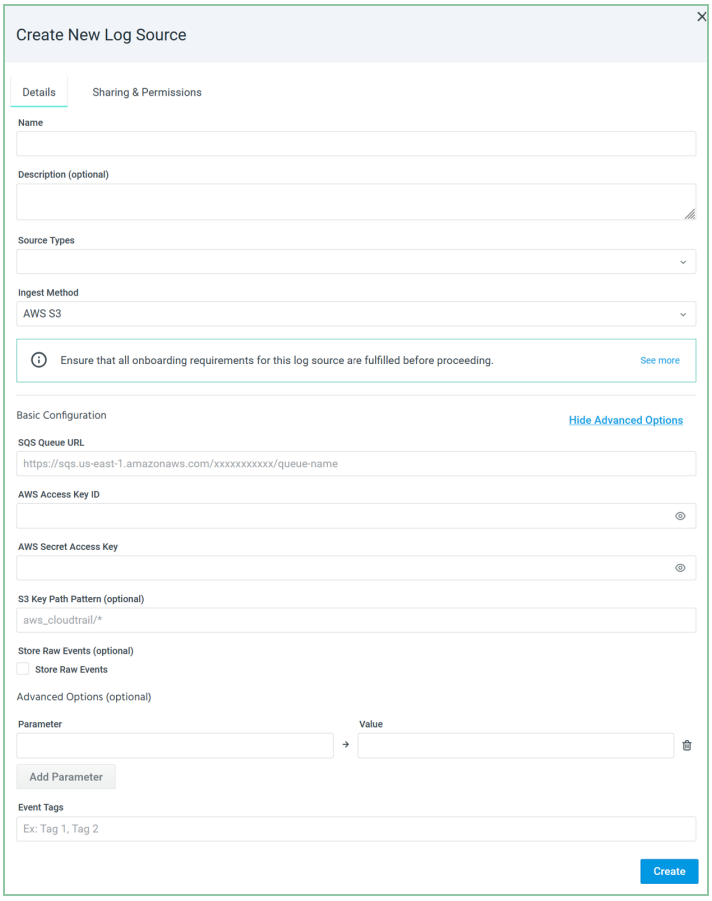
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Cisco ESA Bounce as new log source



On the Anomali platform, add Cisco ESA Bounce as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `cisco_esa_bounce/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"cisco_esa_bounce"` is correct, however `"cisco esa bounce"` is incorrect.

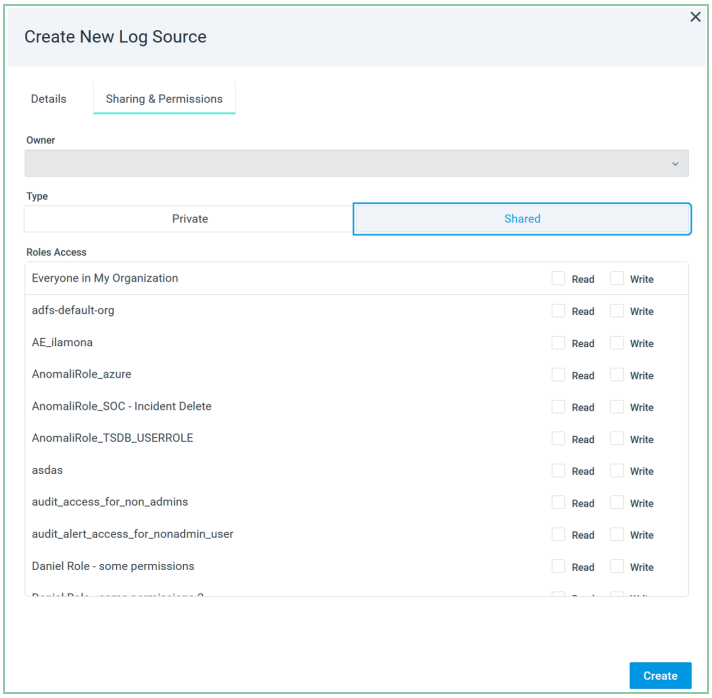
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Cisco ESA CLI Audit

Anomali supports the ingestion of Cisco ESA CLI Audit logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

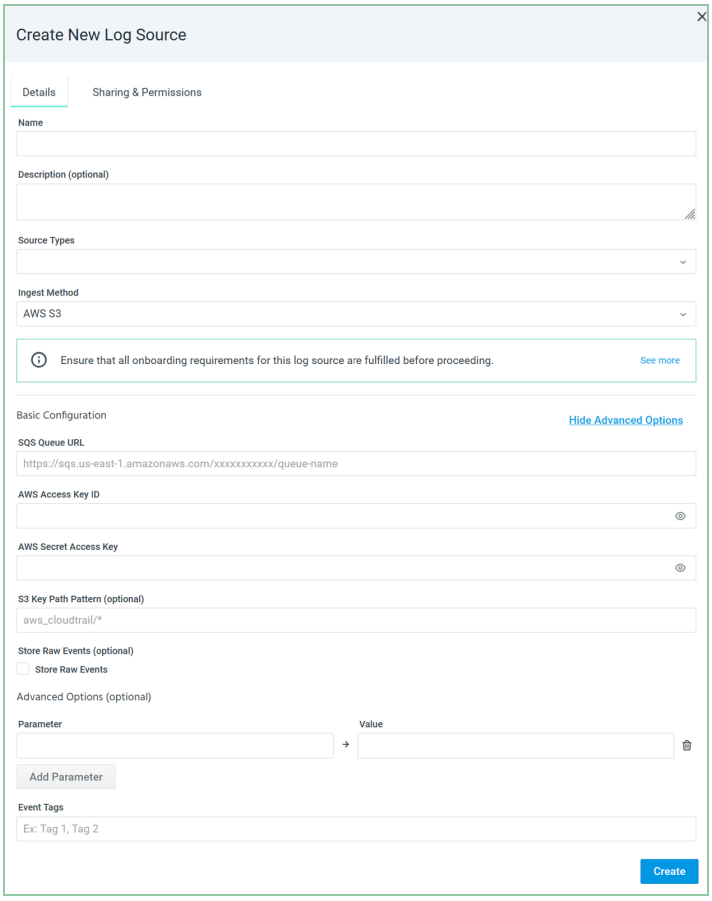
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Cisco ESA CLI Audit as new log source



On the Anomali platform, add Cisco ESA CLI Audit as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `cisco_esa_cli_audit/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"cisco_esa_cli_audit"` is correct, however `"cisco esa cli audit"` is incorrect.

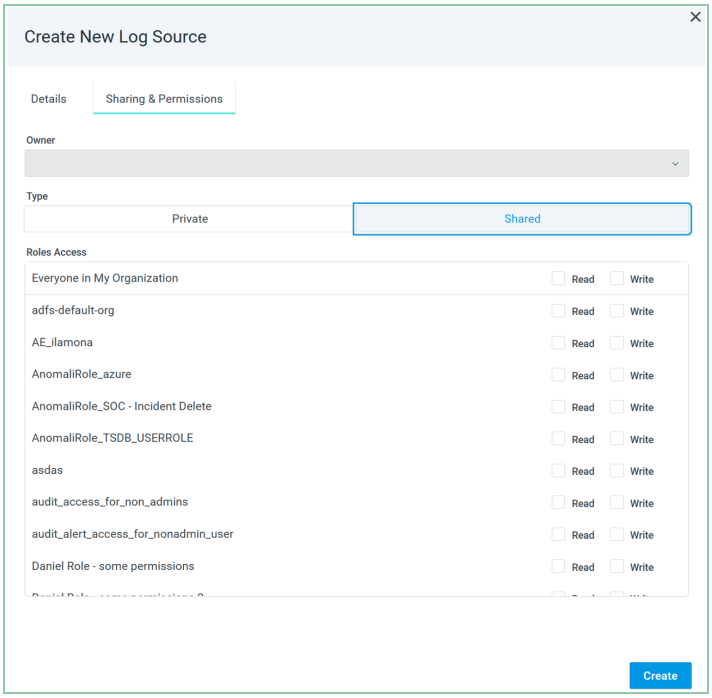
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Cisco ESA Greymail

Anomali supports the ingestion of Cisco ESA Greymail logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

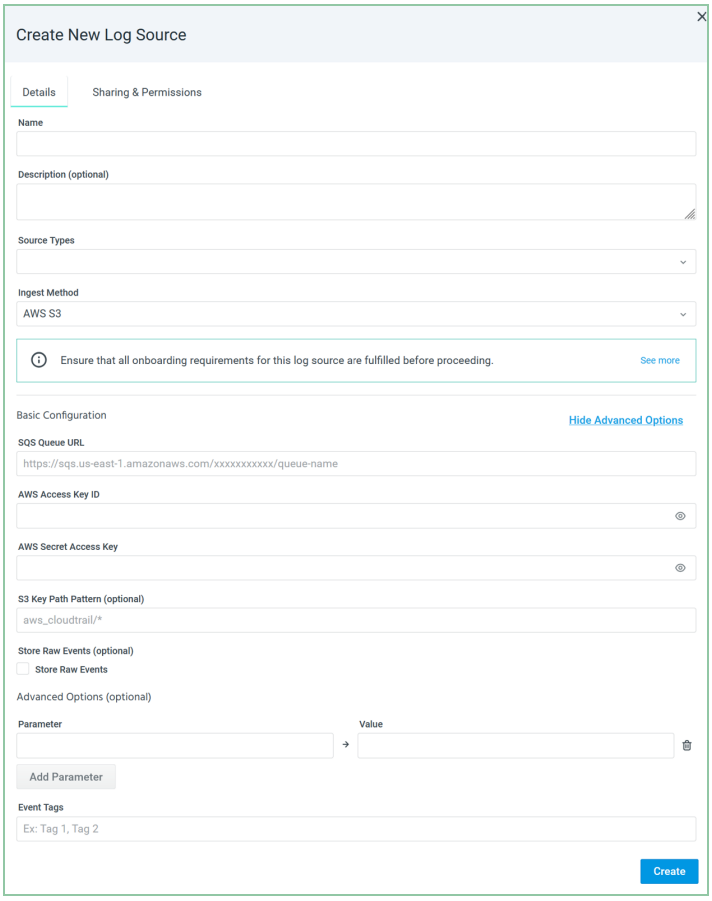
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Cisco ESA Greymail as new log source



On the Anomali platform, add Cisco ESA Greymail as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `cisco_esa_greymail/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"cisco_esa_greymail"` is correct, however `"cisco esa greymail"` is incorrect.

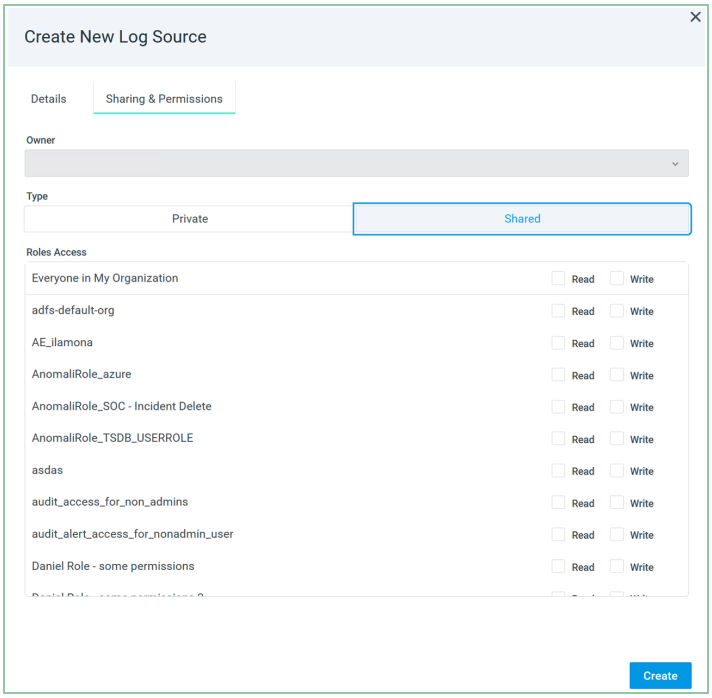
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Cisco ESA HTTP

Anomali supports the ingestion of Cisco ESA HTTP logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

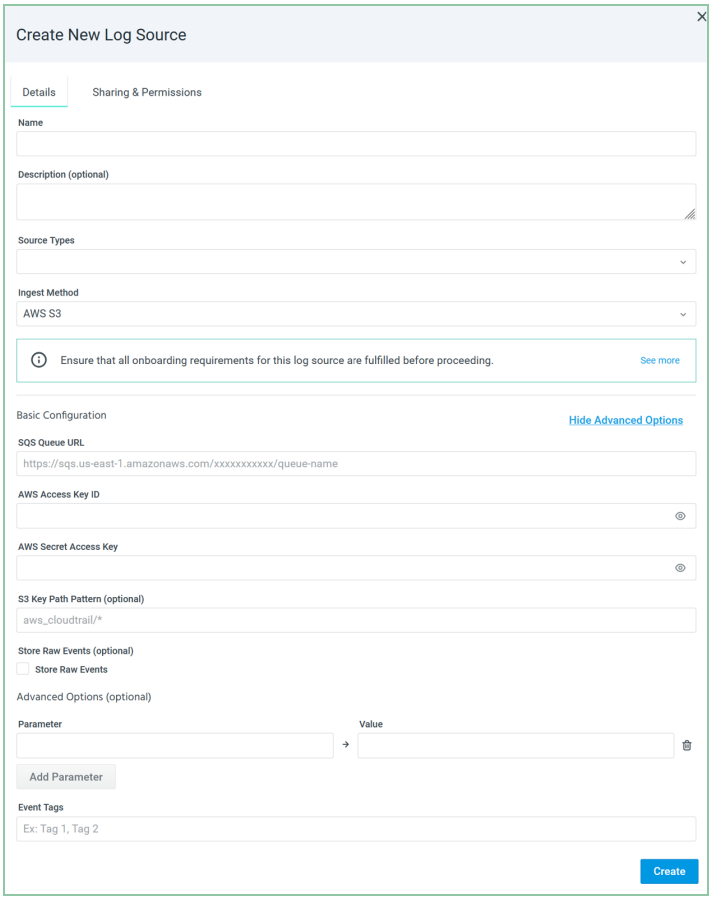
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Cisco ESA HTTP as new log source



On the Anomali platform, add Cisco ESA HTTP as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `cisco_esa_http/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"cisco_esa_http"` is correct, however `"cisco esa http"` is incorrect.

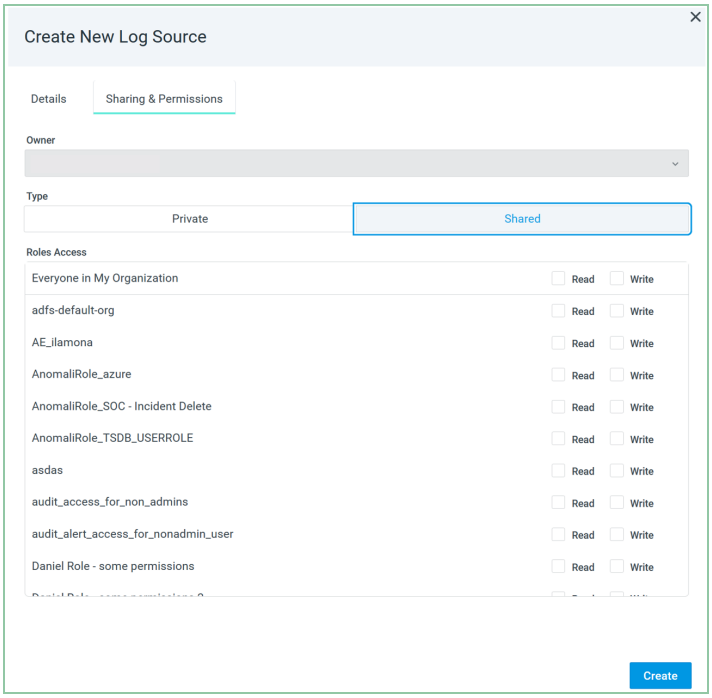
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Cisco ESA LDAP

Anomali supports the ingestion of Cisco ESA LDAP logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

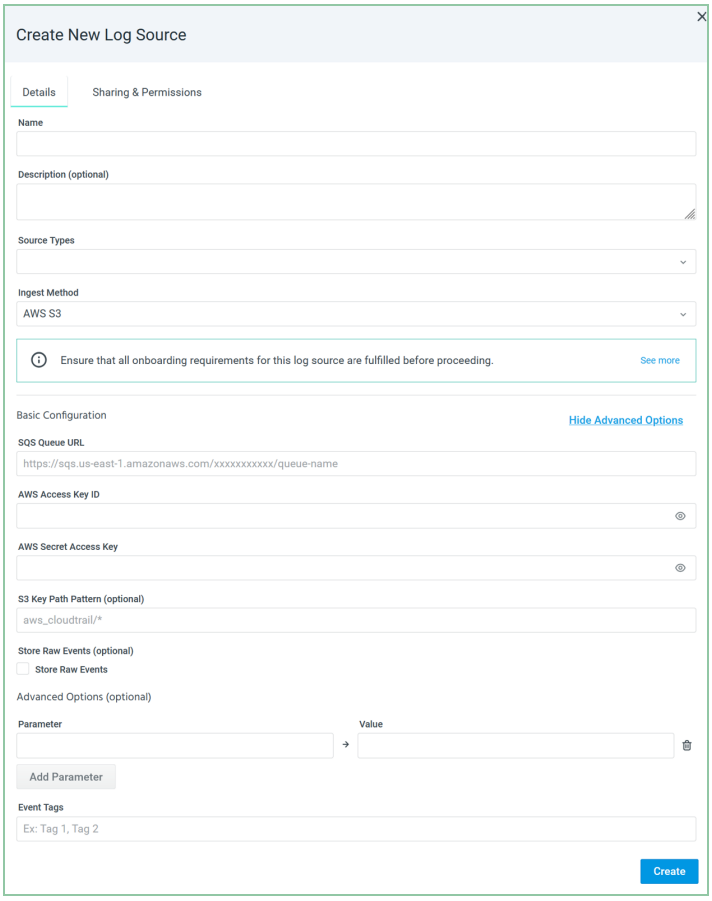
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Cisco ESA LDAP as new log source



On the Anomali platform, add Cisco ESA LDAP as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `cisco_esa_ldap/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"cisco_esa_ldap"` is correct, however `"cisco esa ldap"` is incorrect.

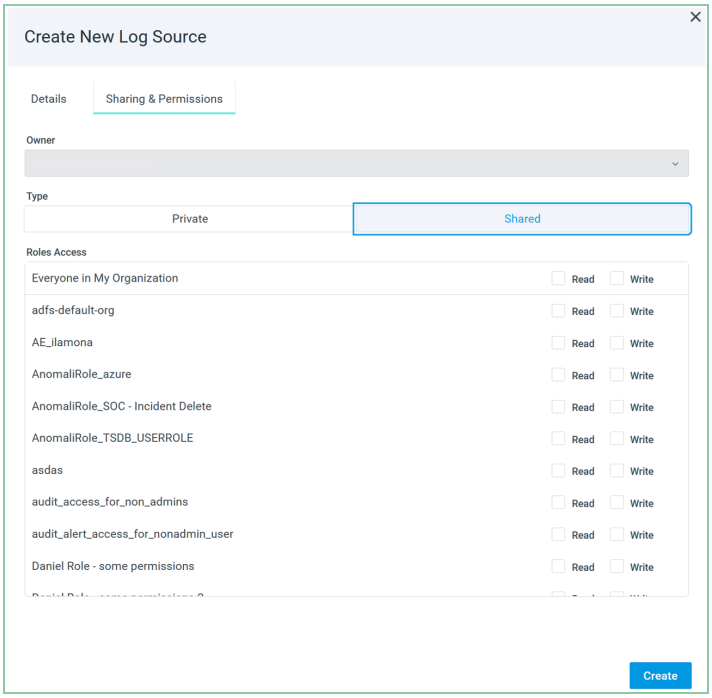
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Cisco ESA NTP

Anomali supports the ingestion of Cisco ESA NTP logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

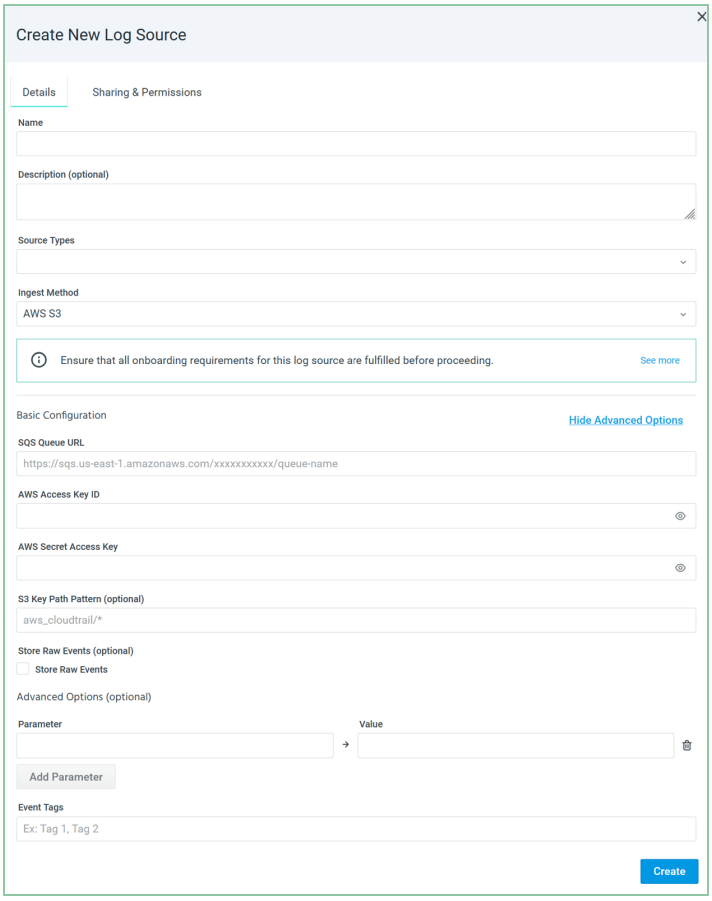
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Cisco ESA NTP as new log source



On the Anomali platform, add Cisco ESA NTP as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `cisco_esa_ntp/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"cisco_esa_ntp"` is correct, however `"cisco esa ntp"` is incorrect.

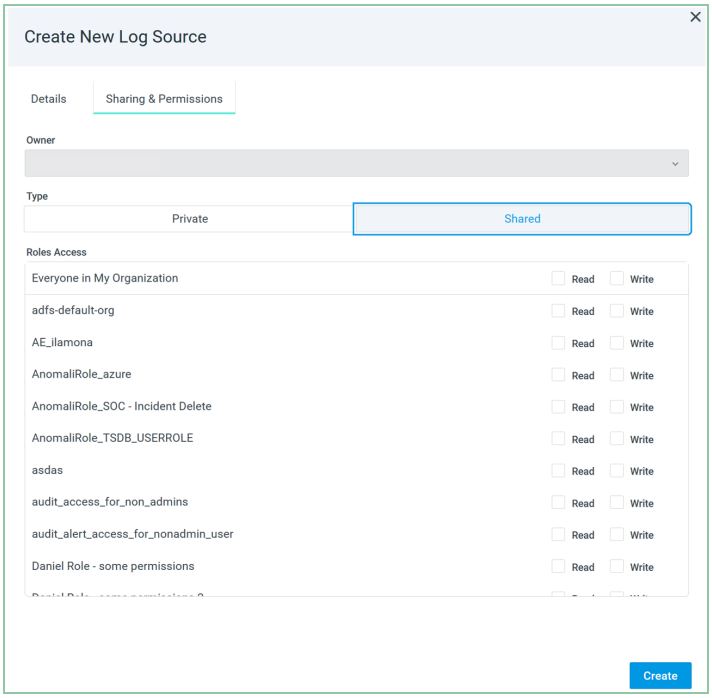
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Cisco ESA Quarantine GUI

Anomali supports the ingestion of Cisco ESA Quarantine GUI logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

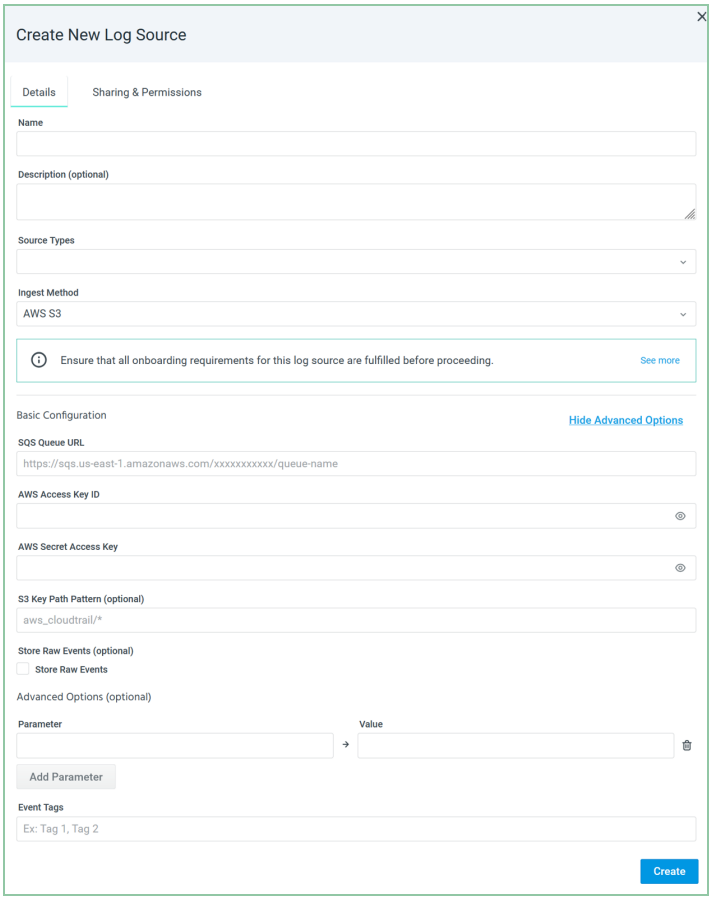
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Cisco ESA Quarantine GUI as new log source



On the Anomali platform, add Cisco ESA Quarantine GUI as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `cisco_esa_quarantine/year=2025/month=03/day=22/events/event_data_logs/`.

- Sourcetype name must not contain any spaces: For example, `"cisco_esa_quarantine"` is correct, however `"cisco esa quarantine"` is incorrect.

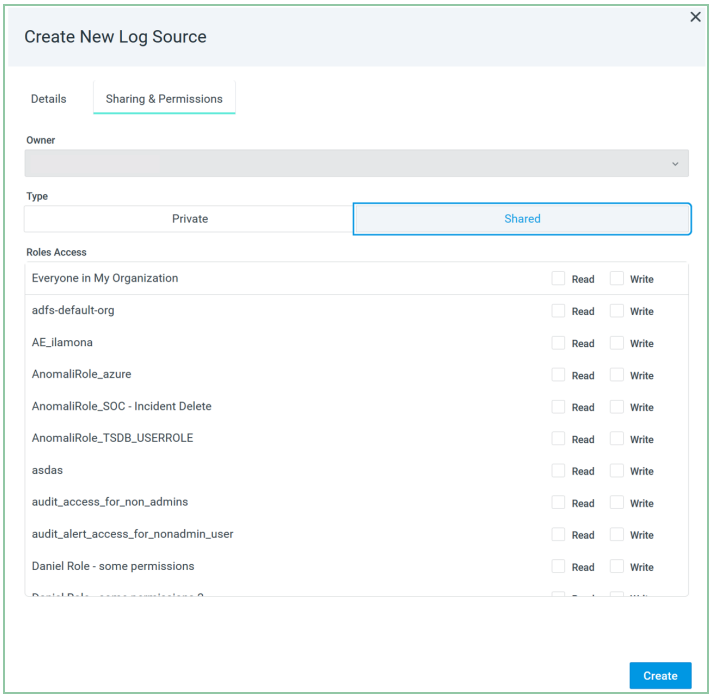
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Cisco ESA Reporting

Anomali supports the ingestion of Cisco ESA Reporting logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

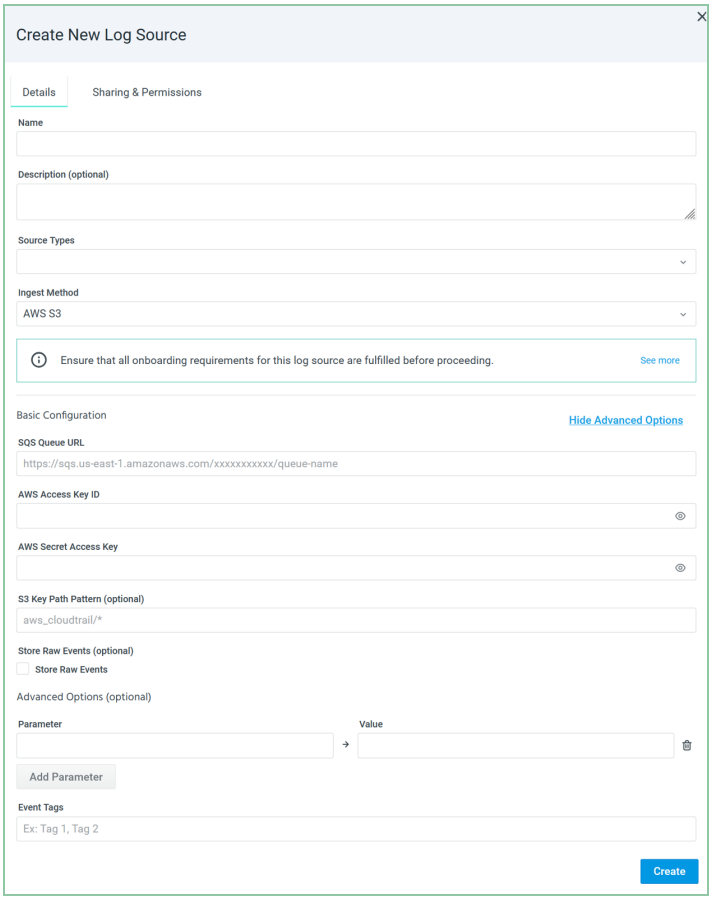
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Cisco ESA Reporting as new log source



On the Anomali platform, add Cisco ESA Reporting as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `cisco_esa_reporting/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"cisco_esa_reporting"` is correct, however `"cisco esa reporting"` is incorrect.

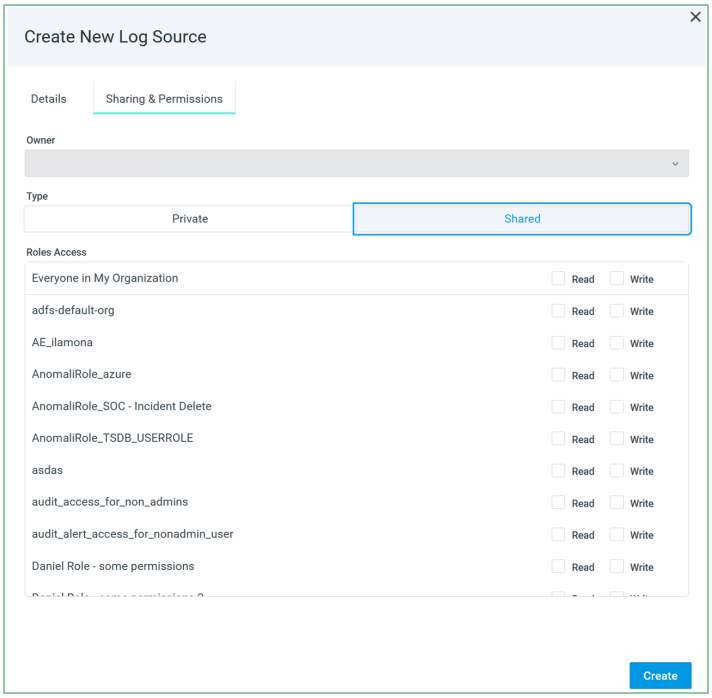
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Cisco ESA Scanning

Anomali supports the ingestion of Cisco ESA Scanning logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

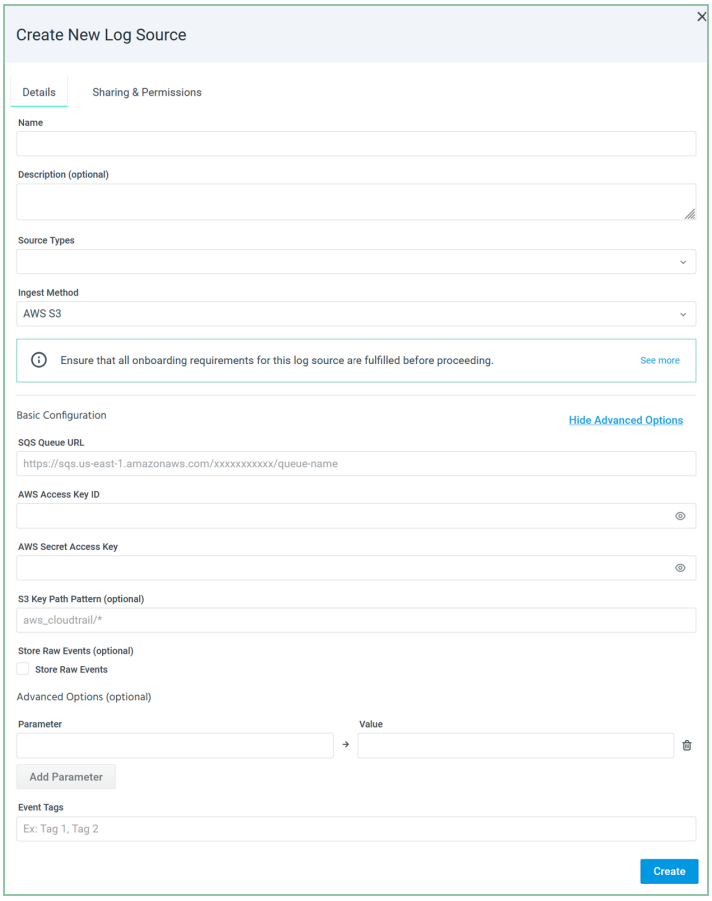
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Cisco ESA Scanning as new log source



On the Anomali platform, add Cisco ESA Scanning as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `cisco_esa_scanning/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"cisco_esa_scanning"` is correct, however `"cisco esa scanning"` is incorrect.

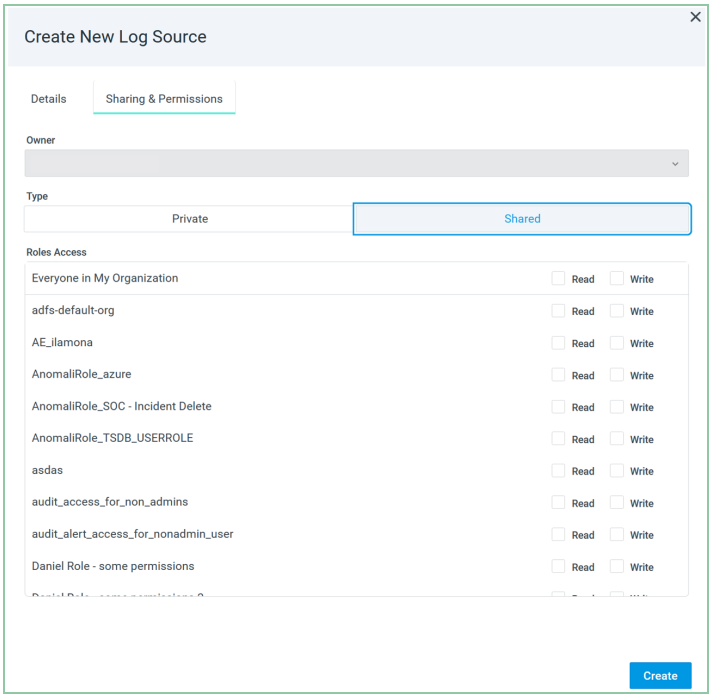
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Cisco ESA Textmail

Anomali supports the ingestion of Cisco ESA Textmail logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

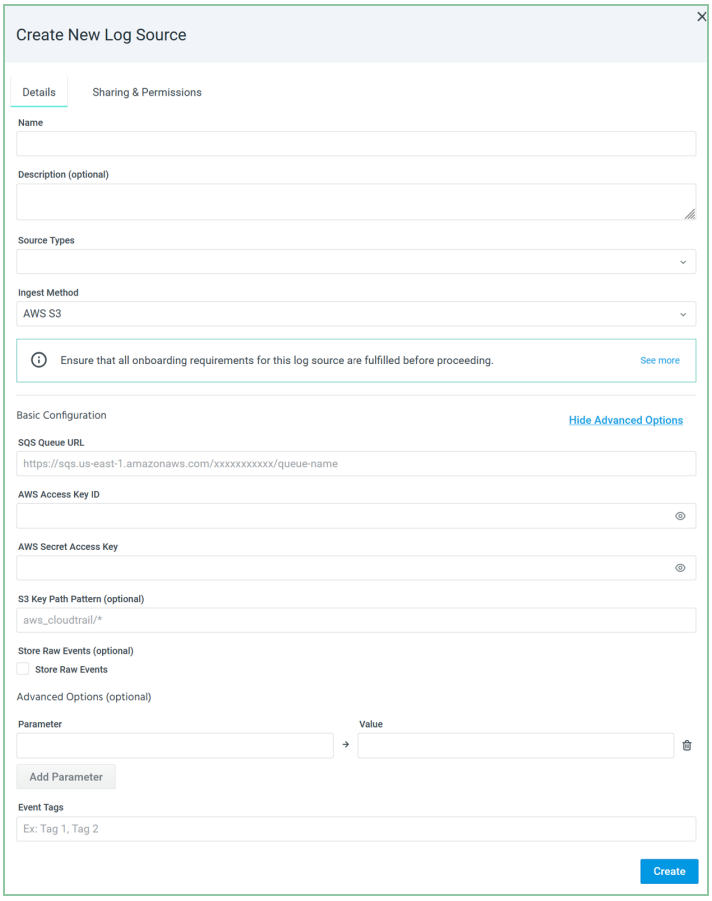
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Cisco ESA Textmail as new log source



On the Anomali platform, add Cisco ESA Textmail as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `cisco_esa_textmail/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"cisco_esa_textmail"` is correct, however `"cisco esa textmail"` is incorrect.

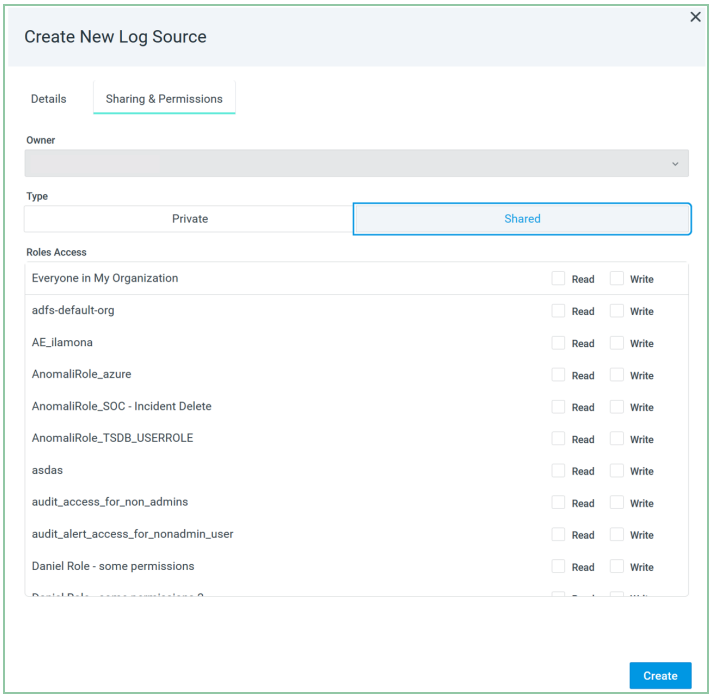
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Cisco FTD

Anomali supports the ingestion of Cisco Firewall Threat Defense (FTD) logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

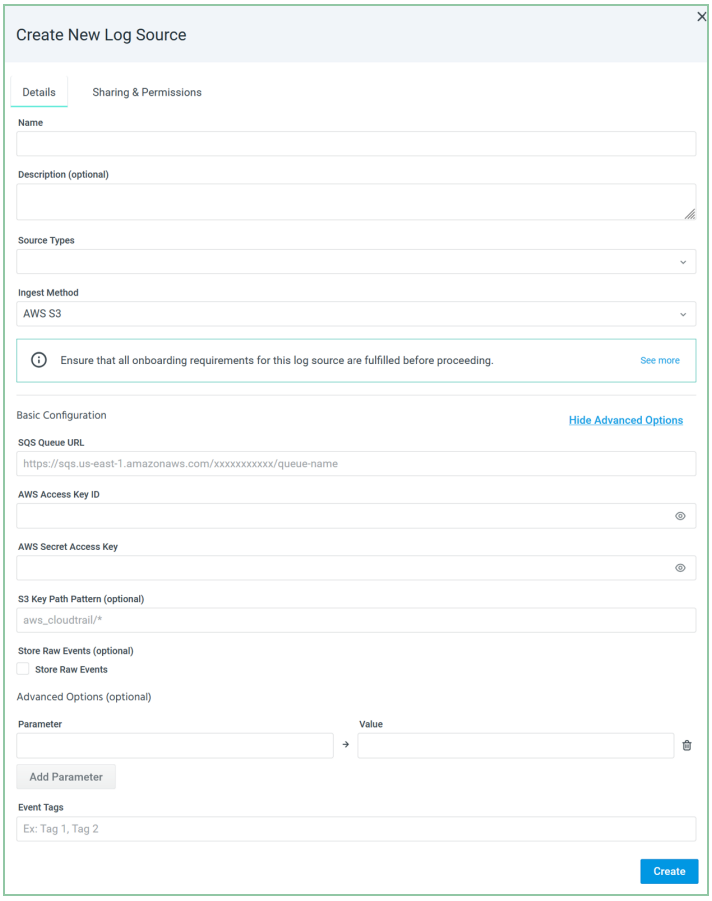
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Cisco FTD as new log source



On the Anomali platform, add Cisco FTD as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `cisco_ftd/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"cisco_ftd"` is correct, however `"cisco ftd"` is incorrect.

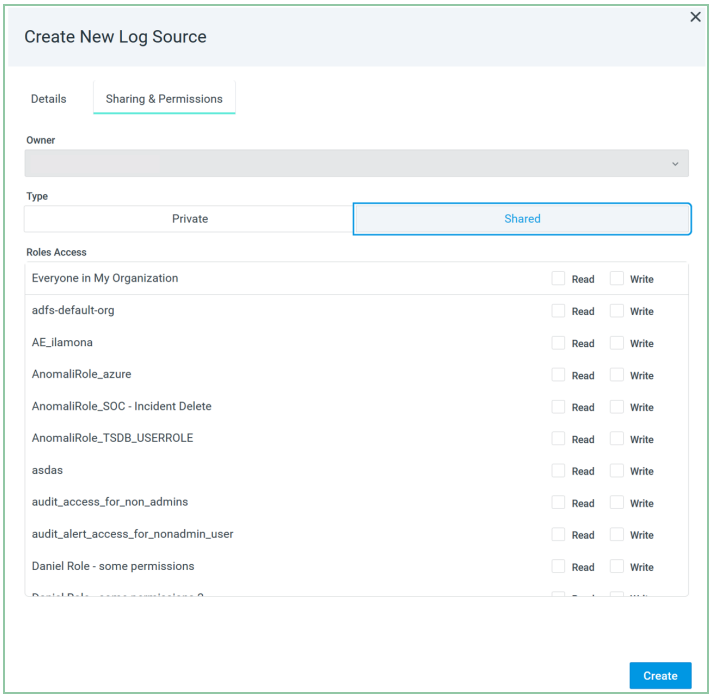
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Cisco Ironport

Anomali supports the ingestion of Cisco Ironport logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

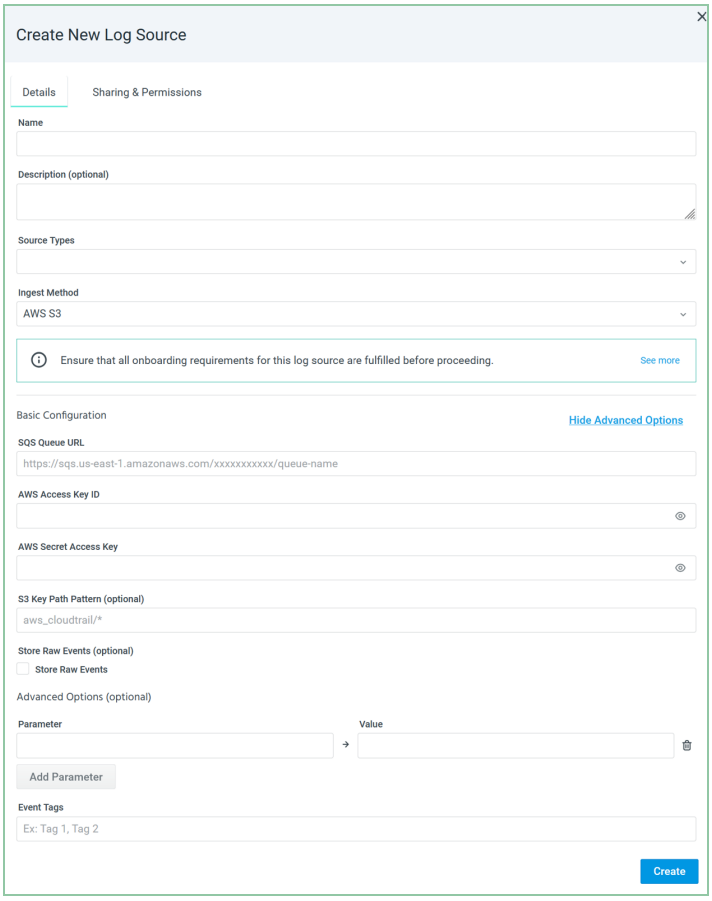
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Cisco Ironport as new log source



On the Anomali platform, add Cisco Ironport as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `cisco_ironport/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"cisco_ironport"` is correct, however `"cisco ironport"` is incorrect.

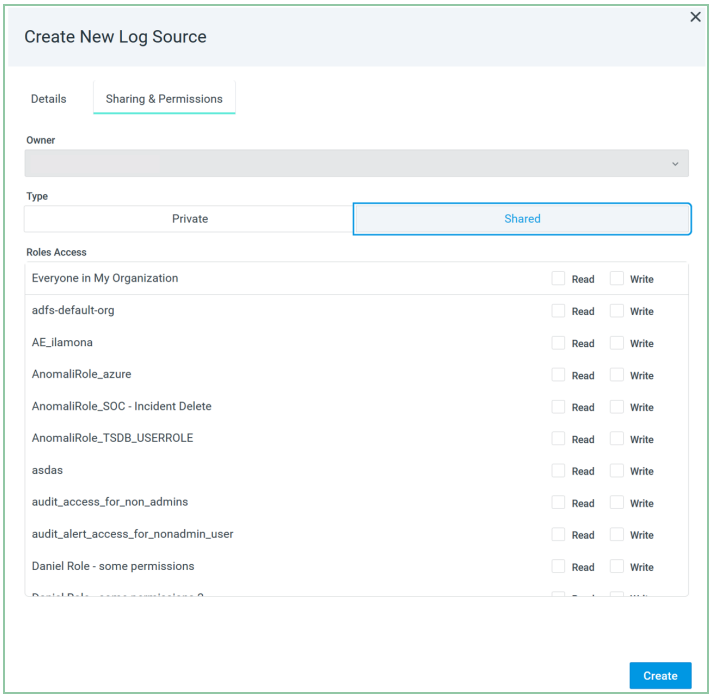
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Cisco ISE

Anomali supports the ingestion of Cisco ISE logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

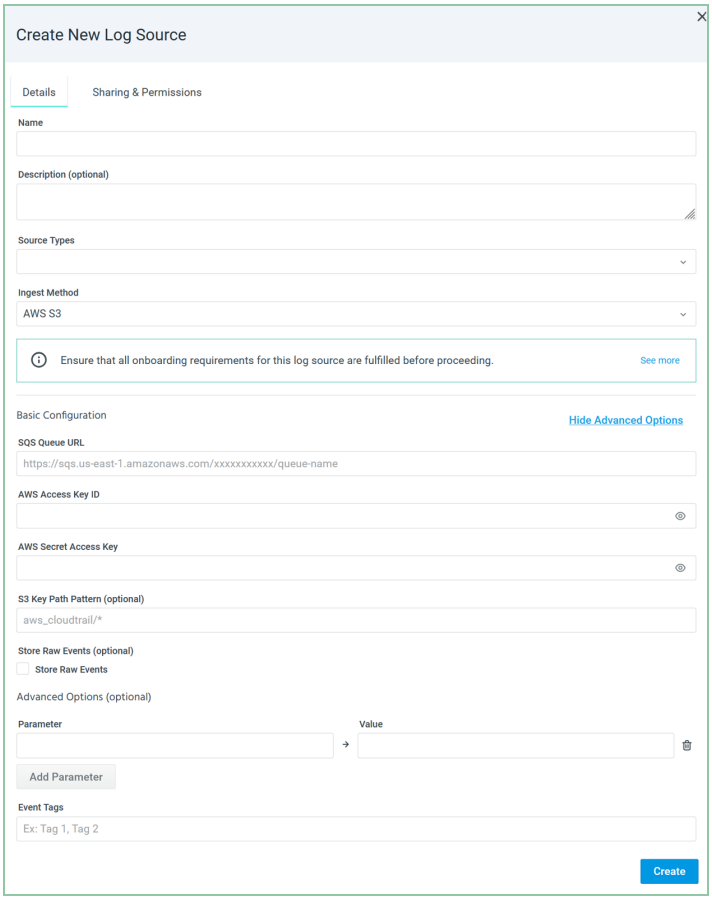
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Cisco ISE as new log source



On the Anomali platform, add Cisco ISE as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `cisco_ise/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"cisco_ise"` is correct, however `"cisco ise"` is incorrect.

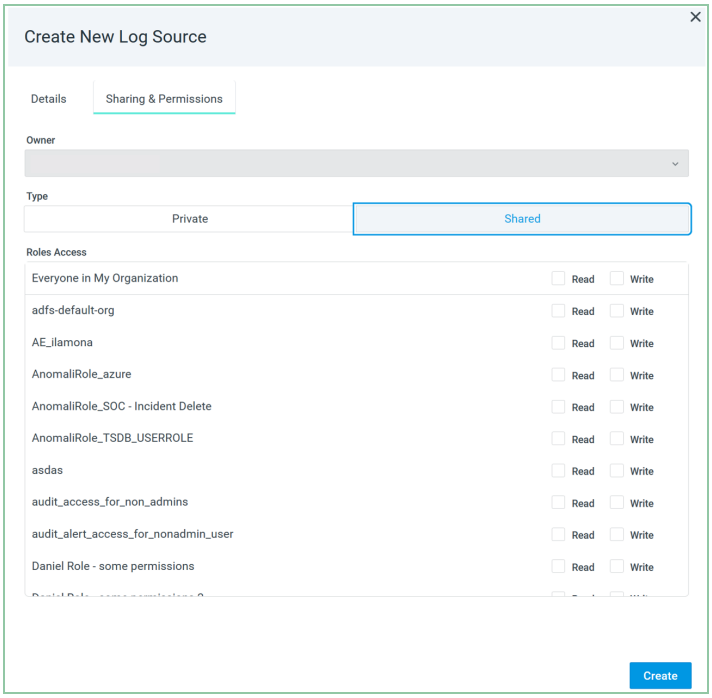
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Cisco Meraki

Anomali supports the ingestion of Cisco Meraki logs through the "Dashboard API" below and AWS S3.

Dashboard API

You can use your existing API token or create a new token to add a new log source in the Anomali platform.

Onboarding steps

Step 1: Create API key

1. Sign into your Cisco Meraki dashboard.
2. Click **My profile** in the top-right corner of the dashboard.
3. Scroll to the API access section, and click **Generate new API key**. Securely store the key value for the subsequent steps.

Step 2: Add Cisco Meraki as new log source

To add Cisco Meraki as a new log source on the Anomali platform:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select **Cisco Meraki** as the source type.
6. Select **API** as the ingestion method.
7. Select API as the ingest method.
8. Provide the Basic Configuration details:
    a. **Token**: Enter your existing token ID or the new token you created in "Step 1: Create API key" above.

b. **Enabled product types**: Enter the product types whose data you would like to ingest into Anomali.

c. **Cisco Meraki domain**: Enter the Cisco Meraki domain name.

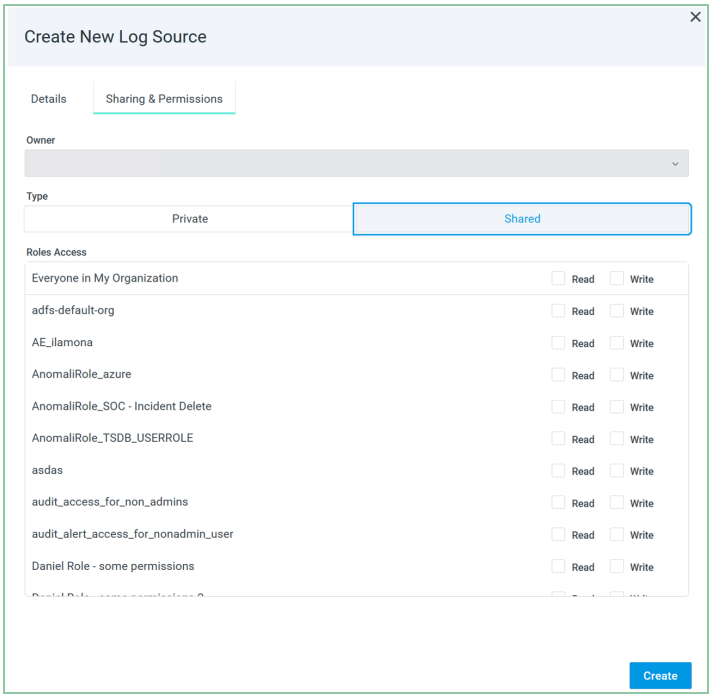
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 3: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 4: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 5: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

AWS S3

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" on the next page. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

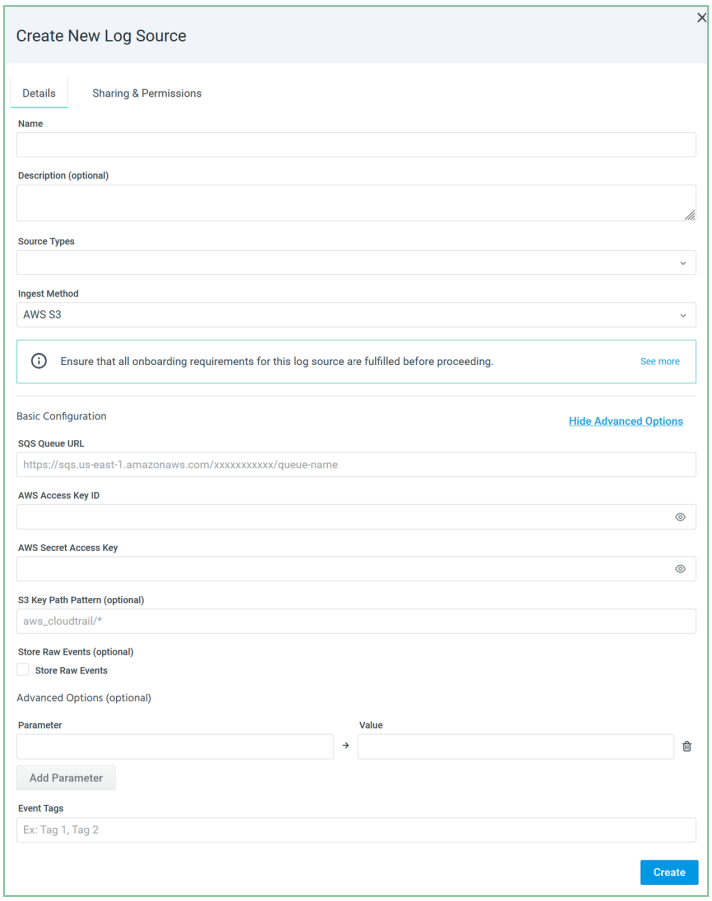
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Cisco Meraki as new log source

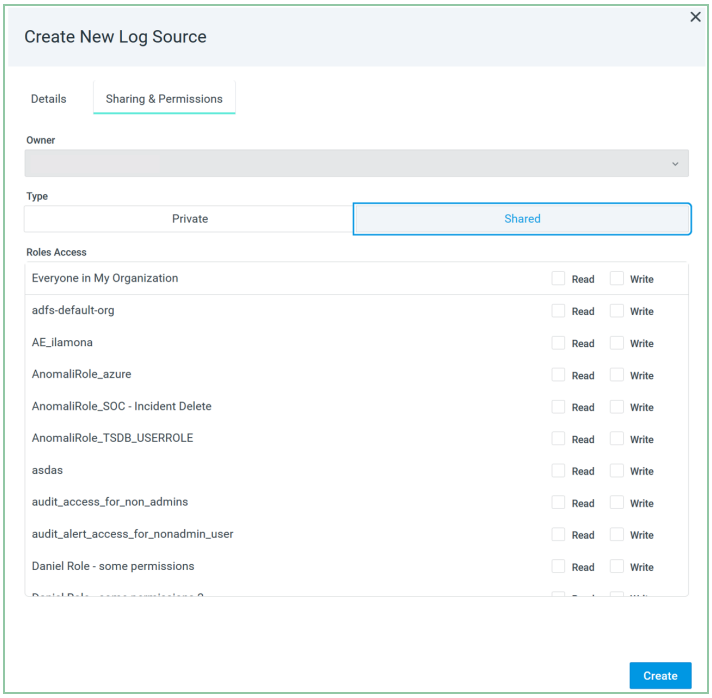


On the Anomali platform, add Cisco Meraki as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.

3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:
   a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.
   b. **AWS Secret Access Key**: Provide the AWS secret access key.
   c. **AWS Access Key ID**: Enter the AWS Access ID.
   d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:
      - Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `cisco_meraki/year=2025/month=03/day=22/events/event_data_logs/`.
      - Sourcetype name must not contain any spaces: For example, `"meraki"` or `"cisco_meraki"` are correct, however `"Cisco Meraki"` is incorrect.
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:
   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.
   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.
10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Cloudflare WAF

Anomali supports the ingestion of Cloudflare WAF logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

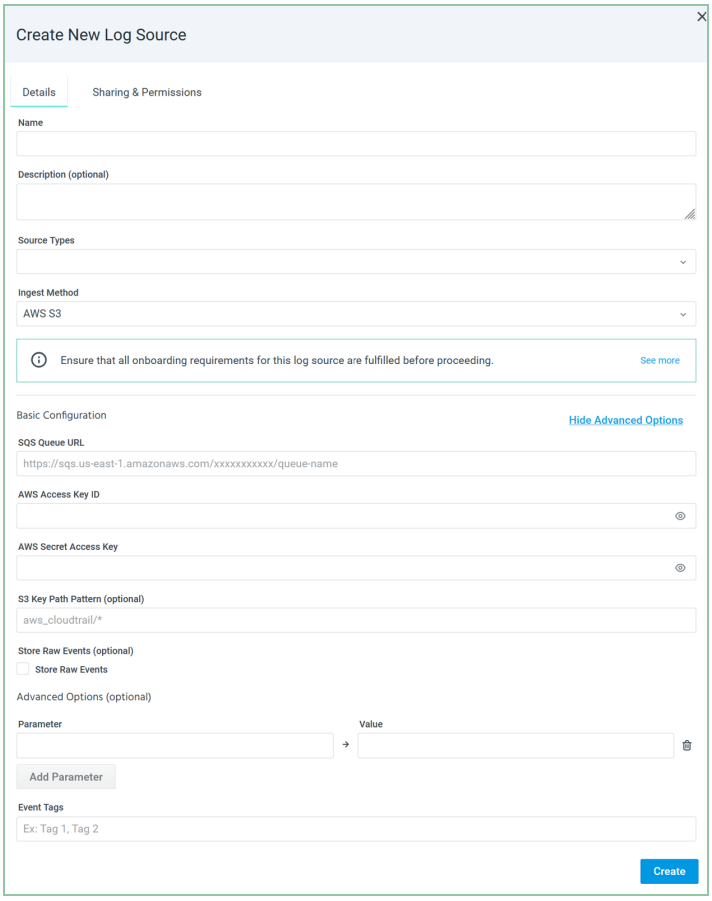
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Cloudflare WAF as new log source



On the Anomali platform, add Cloudflare WAF as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `cloudflare_waf/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"cloudflare_waf"` is correct, however `"cloudflare waf"` is incorrect.

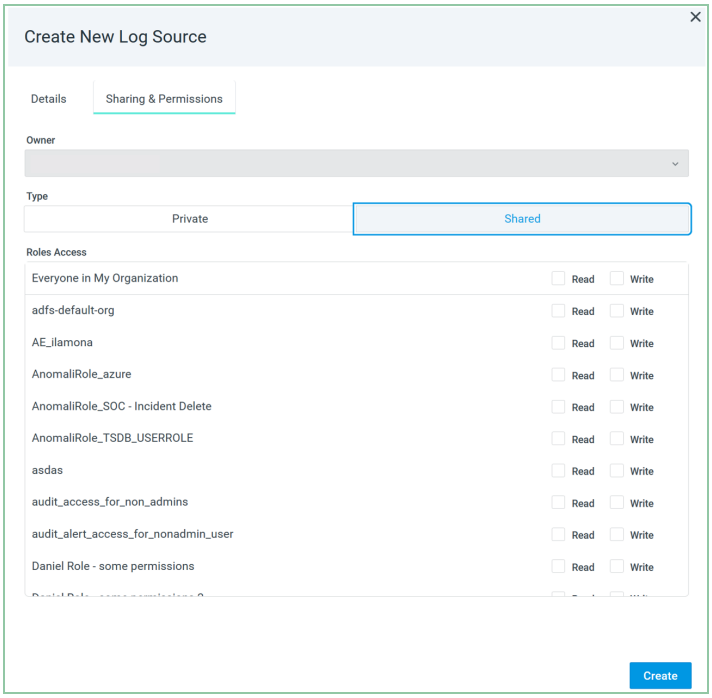
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

CrowdStrike Event Streams

Anomali supports the ingestion of CrowdStrike Event Stream logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

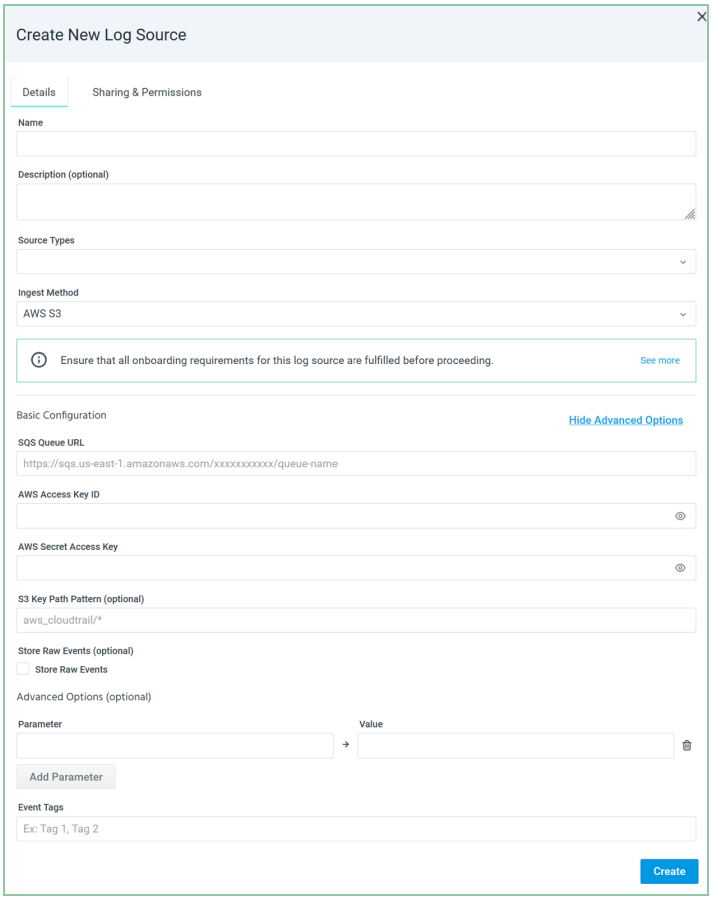
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add CrowdStrike Event Stream as new log source



On the Anomali platform, add CrowdStrike Event Streams as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `crowdstrike_event_streams/year=2025/month=03/day=22/events/event_data_logs/`.

- Sourcetype name must not contain any spaces: For example, `"crowdstrike_event_streams"` is correct, however `"crowdstrike event streams"` is incorrect.

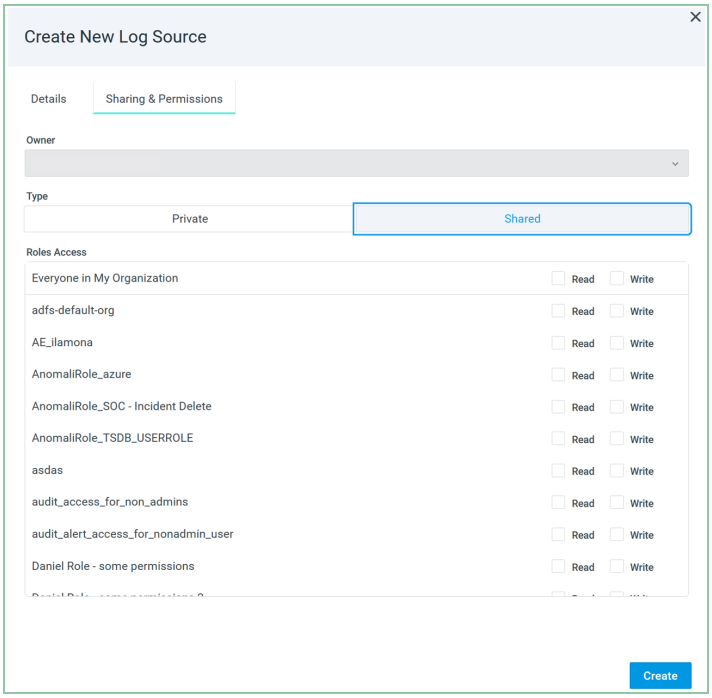
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

CrowdStrike FDR

Anomali supports the ingestion of CrowdStrike Falcon Data Replicator (FDR) logs through AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

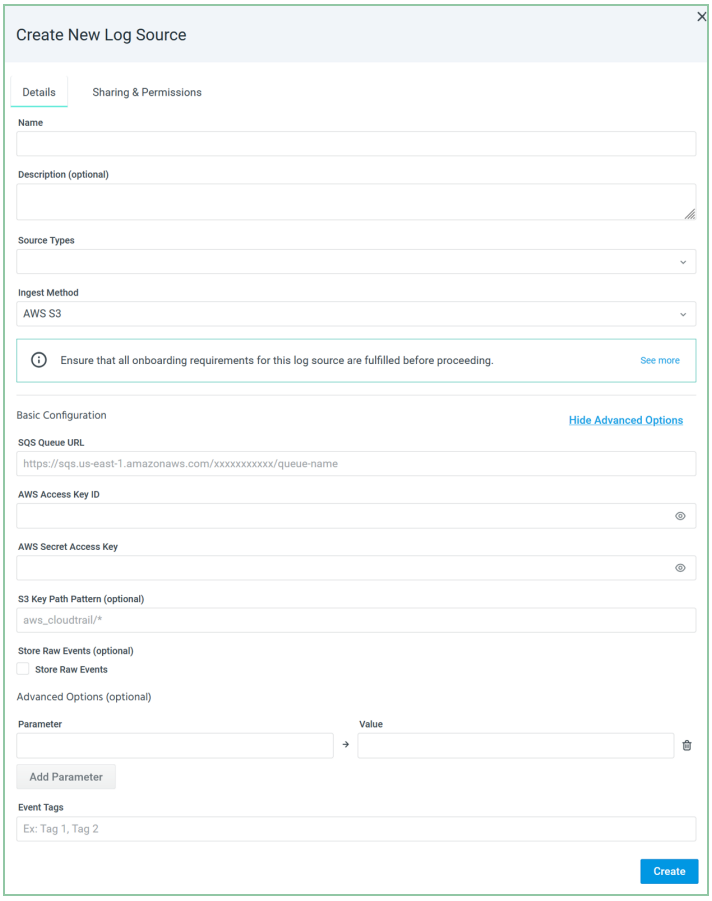
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add CrowdStrike FDR as new log source



On the Anomali platform, add CrowdStrike FDR as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `crowdstrike_fdr/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"crowdstrike_fdr"` is correct, however `"CrowdStrike FDR"` is incorrect.

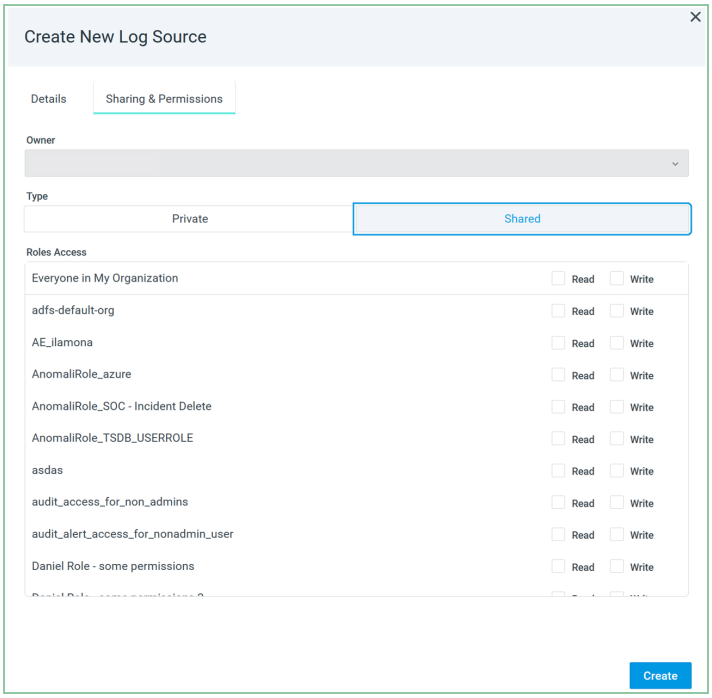
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions

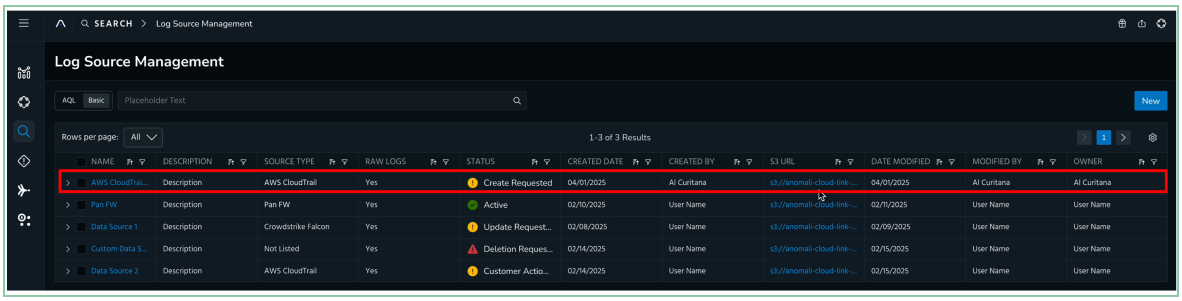


You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.



Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Cyberark EPV

Anomali supports the ingestion of Cyberark EPV logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

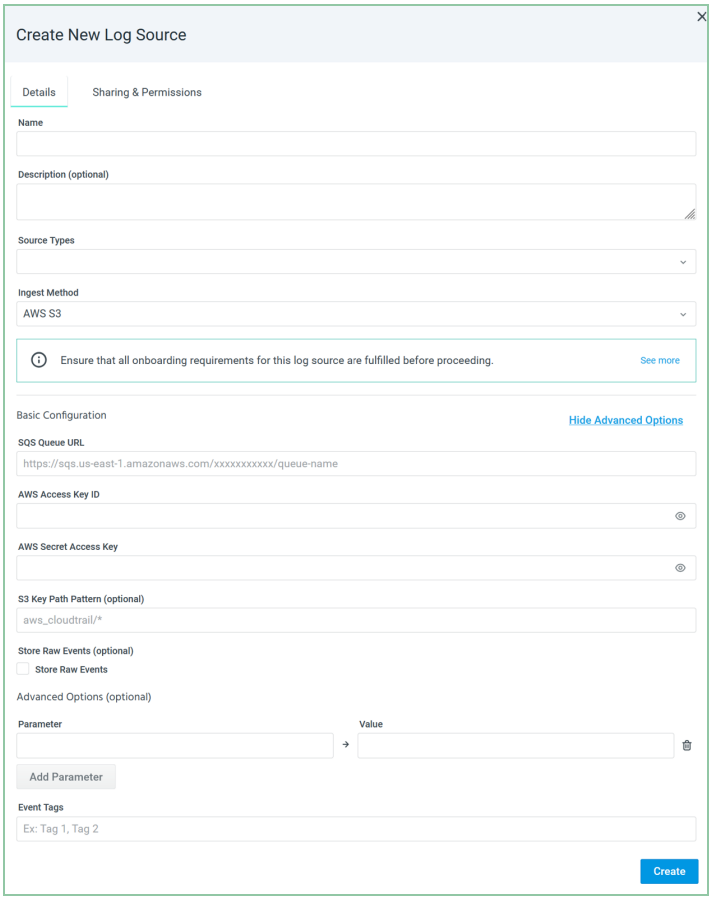
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Cyberark EPV as new log source



On the Anomali platform, add Cyberark EPV as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `cyberark_epv/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"cyberark_epv"` is correct, however `"cyberark EPV"` is incorrect.

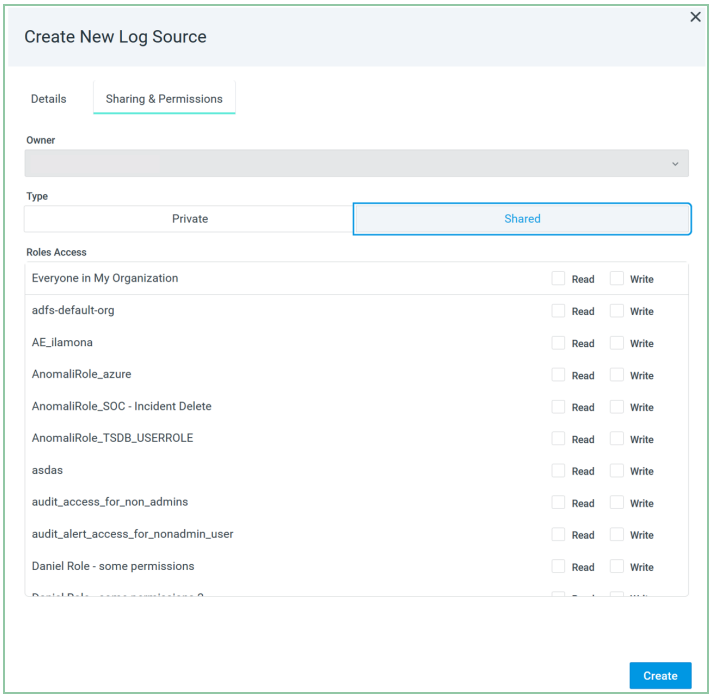
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Microsoft Defender

Anomali supports the ingestion of Microsoft Defender logs. The following article explains the steps you must complete to ingest Microsoft Defender logs into Anomali.

Onboarding steps

Prerequisites

Azure AD requires setting up the Azure Storage Account. Complete Steps 1-2 of Azure Active Directory before you go to "Step 3: Add Defender as new log source" below.

Step 3: Add Defender as new log source

To add Defender as a new log source on the Anomali platform:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select **Defender** as the source type.
6. Select **API** as the ingestion method.
7. Select API as the ingest method.
8. Provide the Basic Configuration details:
    a. **Azure Storage Account Name**: Type the provisioned storage account name from "Microsoft Defender " above.
    b. **Azure Storage Account Access Key**: Paste the key for the provisioned account from "Microsoft Defender " above.
    c. **Wildcard Log Schema**: Provide the wildcard log schema.
    d. (Optional) **Raw events**: Select **Enable** to collect and store the entire event log that is available from the log source.

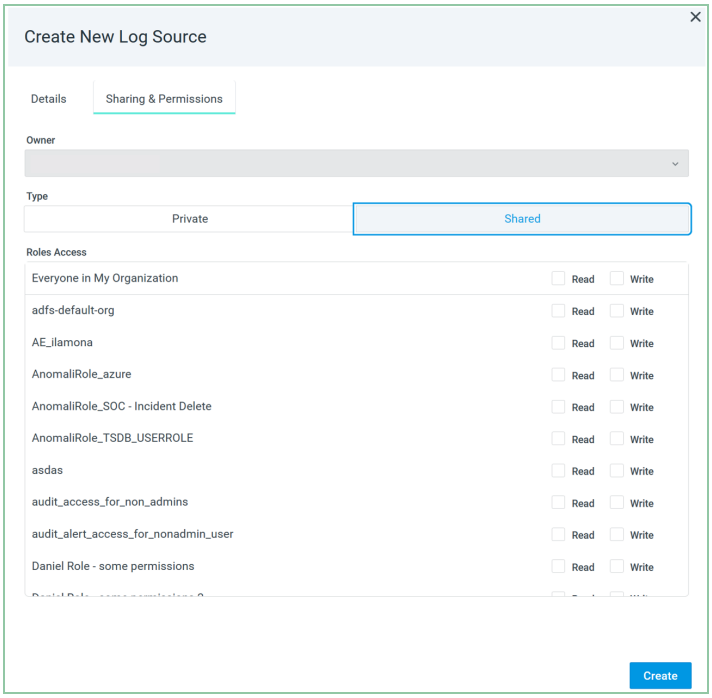
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

    a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

    b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 4: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.

2. Type: Select the type of permission assigned to the view:

    a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.

b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 5: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 6: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

AWS S3

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

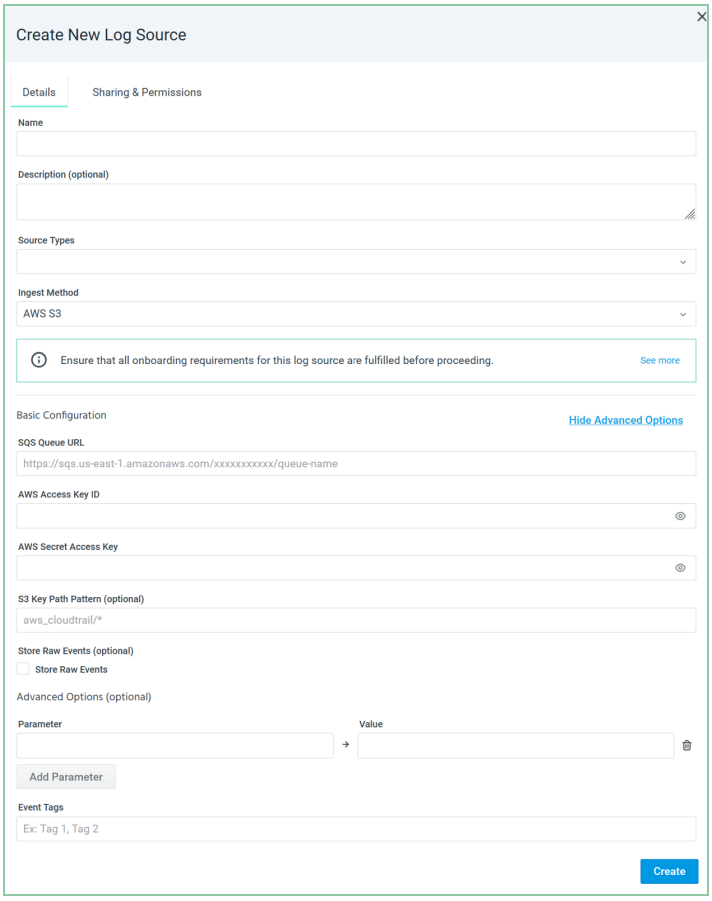
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Defender as new log source



On the Anomali platform, add Defender as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `defender/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"defender"` or `"defender_sourcetype"` are correct, however `"Defender sourcetype"` is incorrect.

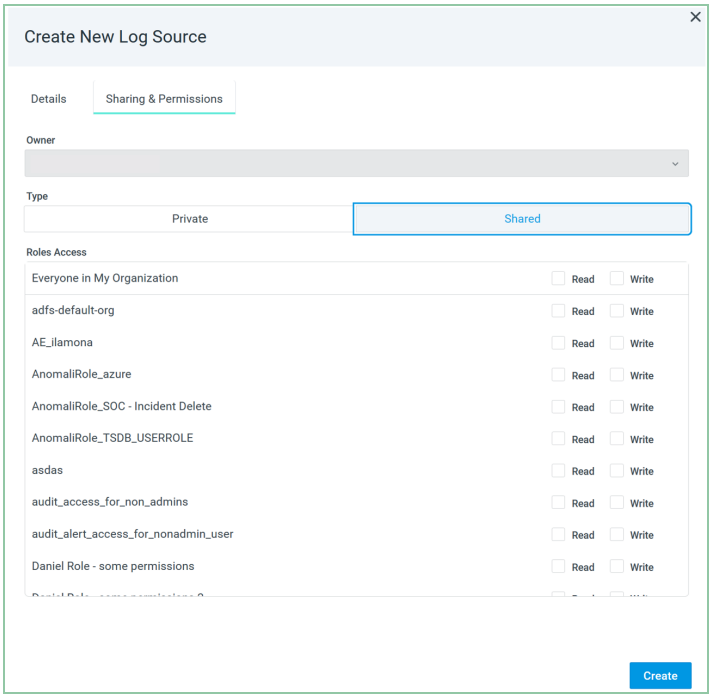
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Microsoft Defender ATP

Anomali supports the ingestion of Microsoft Defender ATP logs. The following article explains the steps you must complete to ingest Defender ATP logs into Anomali.

API call

Prerequisites

1. Your organization must have an active subscription to Azure.
2. Your organization must have a Microsoft 365 E5 license. Refer to the Microsoft website for details.
3. You must deploy Microsoft Endpoint Defender to the hosts you intend to manage. See Microsoft's guide to Onboard devices and configure Microsoft Defender for Endpoint capabilities for details.

Step 1: Create an app

Create a Microsoft Entra ID app. See Microsoft's guide to Create an app for more details.

Step 2: Add permissions

1. On the application page, go to **API Permissions**.
2. Click **Add a permission** > **APIs my organization uses**.
3. Type **WindowsDefenderATP** and select **WindowsDefenderATP**.
4. Select **Application permissions**, select **Alert.Read.All**, and then click **Add permissions**.
5. When prompted, grant admin consent.

On the application page, go to **Overview** and copy the following details to a secure, temporary location you can access when you complete the Security Analytics log source configuration:

- Application (client) ID
- Directory (tenant ID)

Step 3: Add client secret

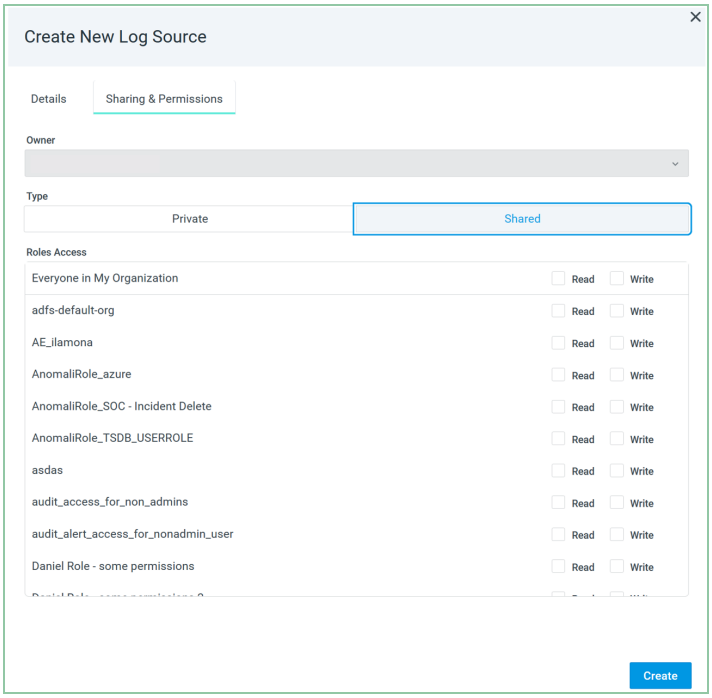
Click **Add a certificate or secret** and complete the workflow to generate an application secret. Securely save this secret for subsequent steps.

Step 4: Add Defender ATP as new log source

To add Defender ATP as a new log source on the Anomali platform:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select **Defender ATP** as the source type.
6. Select **API** as the ingestion method.
7. Select API as the ingest method.
8. Provide the Basic Configuration details:
   a. **Tenant ID**: Enter the tenant ID from "Step 2: Add permissions " on the previous page.
   b. **Client ID**: Enter the client ID from "Step 2: Add permissions " on the previous page.
   c. **Client Secret**: Enter the client secret from "Step 3: Add client secret" on the previous page.
   d. **Get Alerts**: Enabled by default to collect Alert events. Do not enable if you are not interested in Alert events.
   e. (Optional)**Ingestion Interval**: Specify the number of minutes, hours, or days between API requests.
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:
   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.
   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.
10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

AWS S3

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

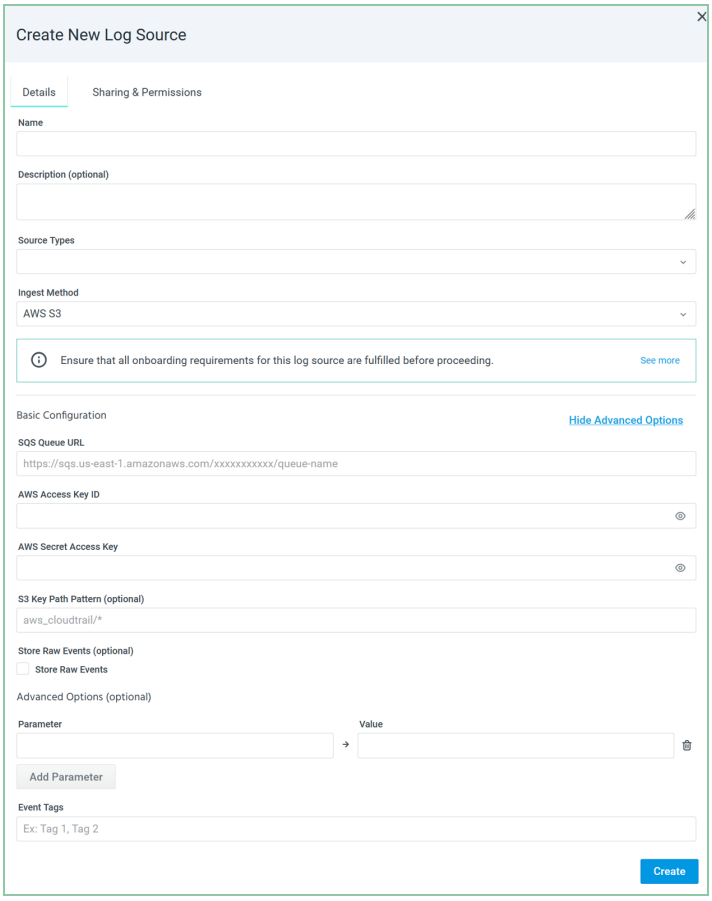
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Defender ATP as new log source



On the Anomali platform, add Defender ATP as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `defender_atp/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"defender_atp"` or `"defender_ATP_sourcetype"` are correct, however `"Defender atp"` is incorrect.

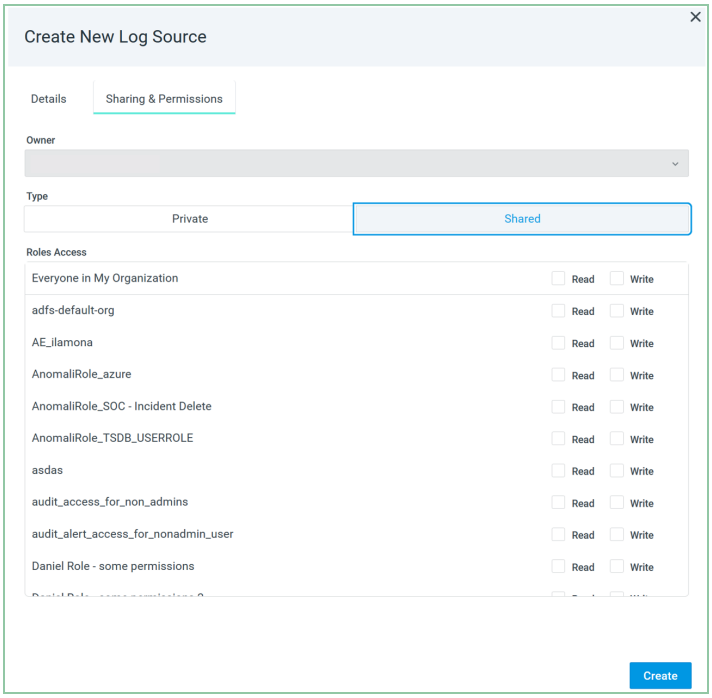
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Duo

Anomali supports the ingestion of Duo logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

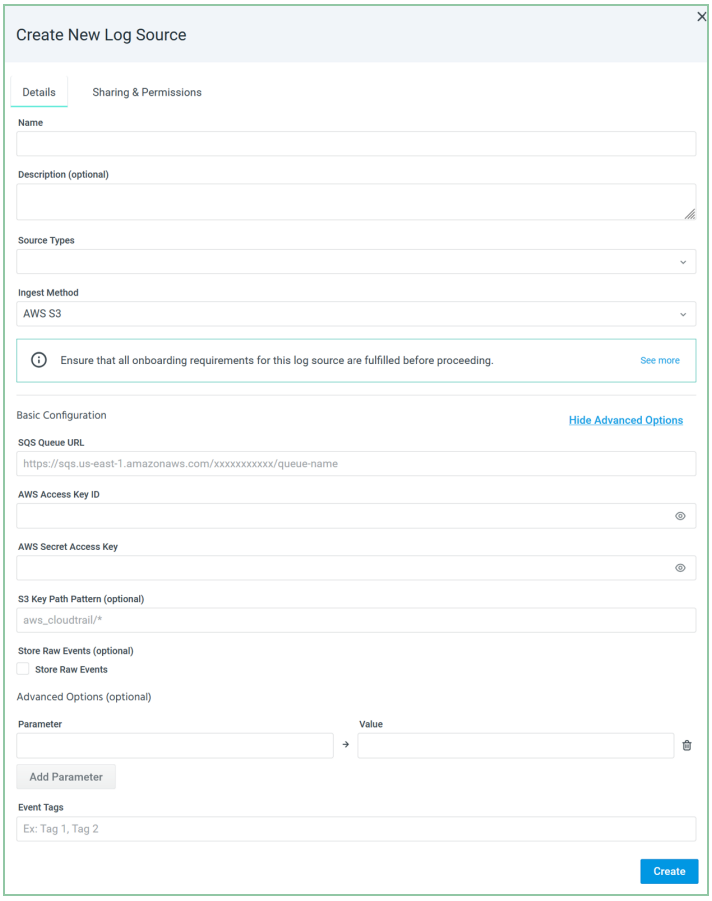
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Duo as new log source



On the Anomali platform, add Duo as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `duo/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"duo_sourcetype"` is correct, however `"duo sourcetype"` is incorrect.

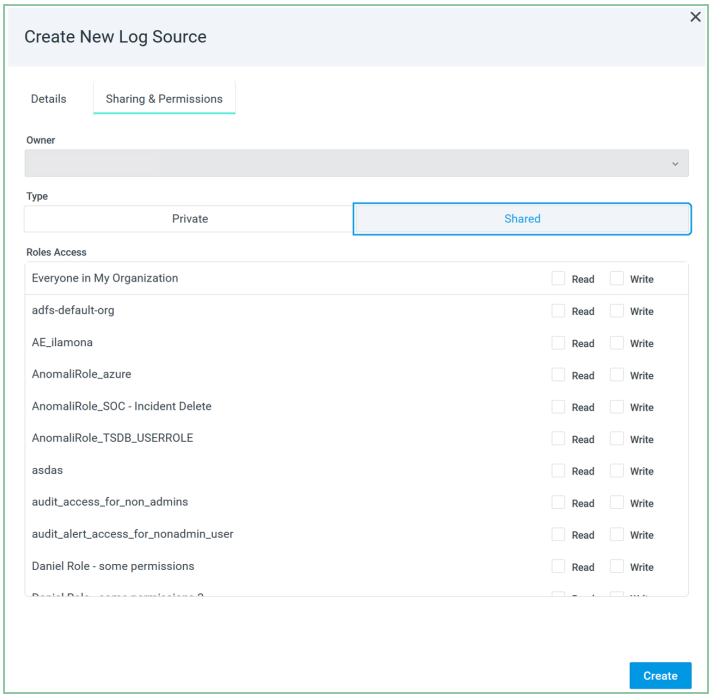
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

ESXi

Anomali supports the ingestion of ESXi logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

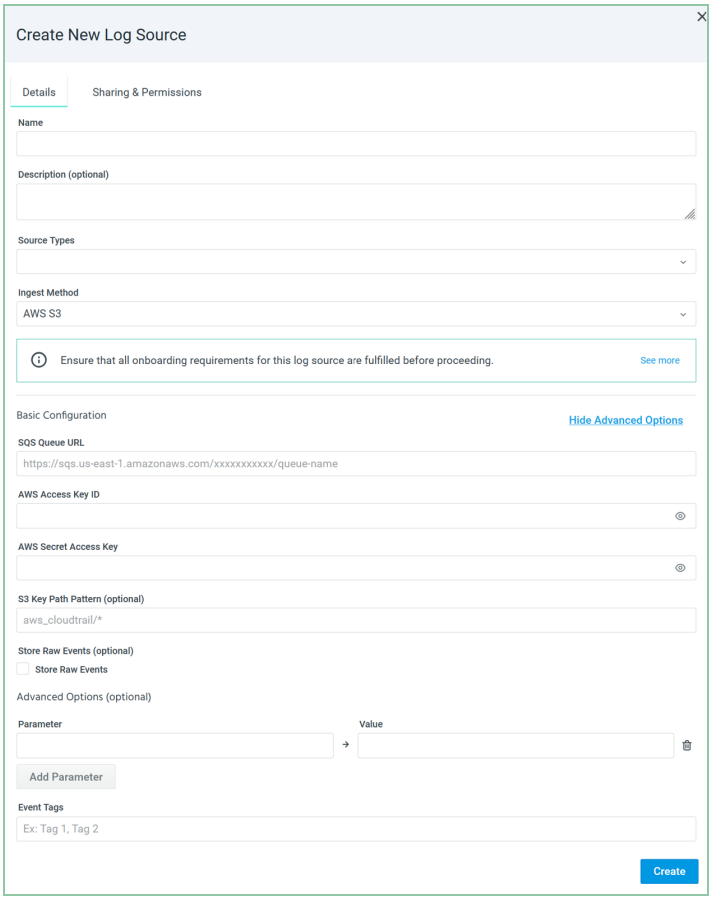
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add ESXi as new log source



On the Anomali platform, add ESXi as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `esxi/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"esxi"` or `"esxi_sourcetype"` correct, however `"esxi sourcetype"` is incorrect.

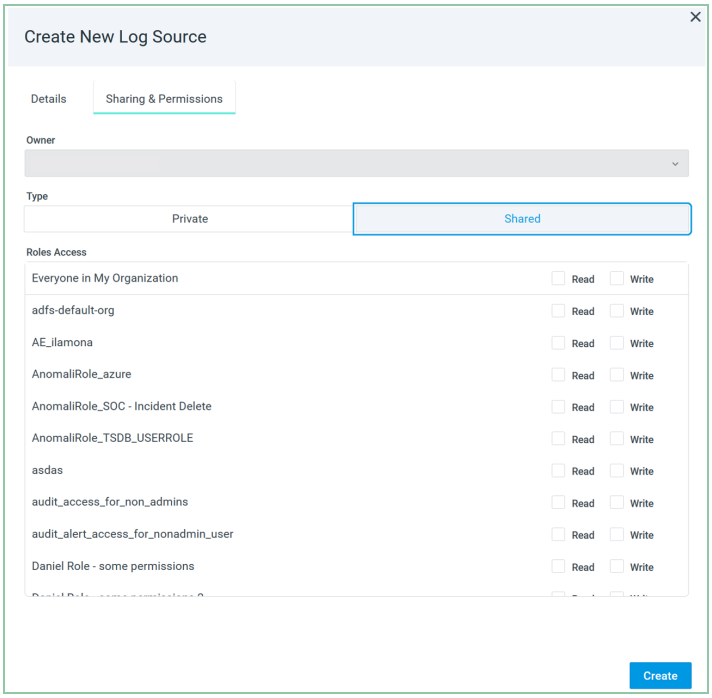
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

F5 BIG-IP

Anomali supports the ingestion of F5 BIG-IP logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

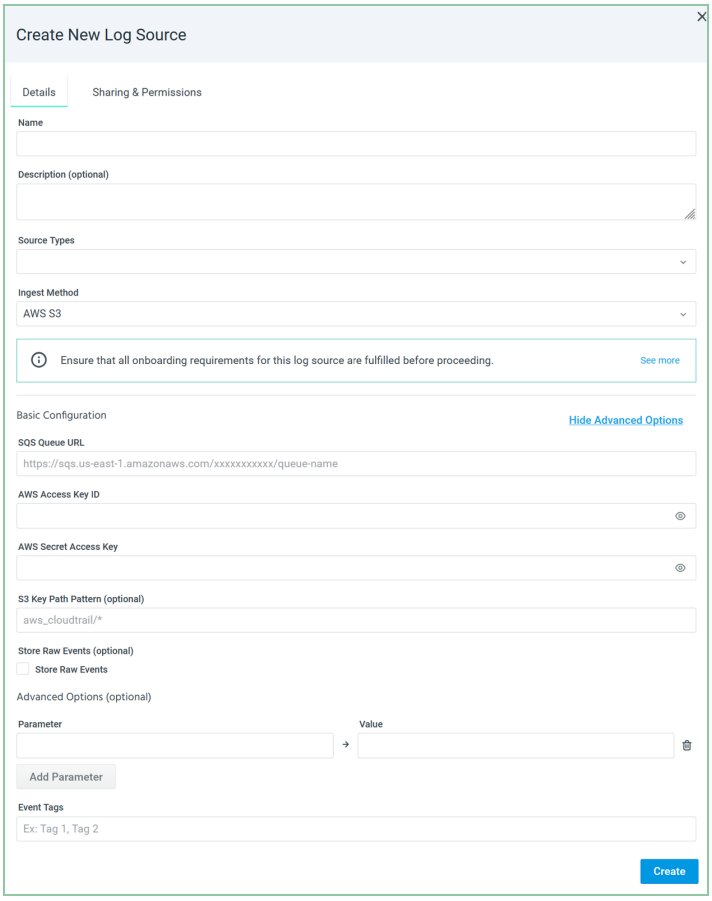
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add F5 BIG-IP as new log source



On the Anomali platform, add F5 BIG-IP as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `f5_big_ip/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"f5_big_ip"` is correct, however `"f5 big ip"` is incorrect.

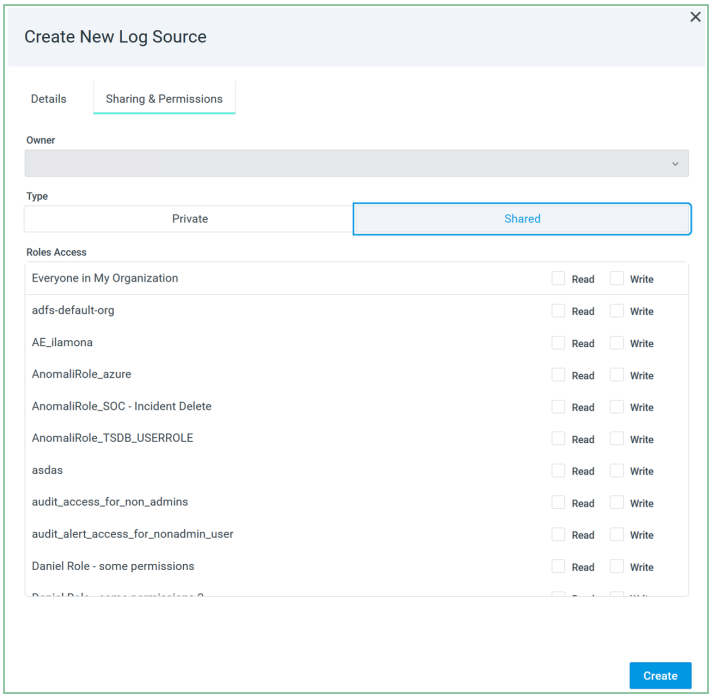
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

F5 BIG-IP TCL Error

Anomali supports the ingestion of F5 BIG-IP TCL Error logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

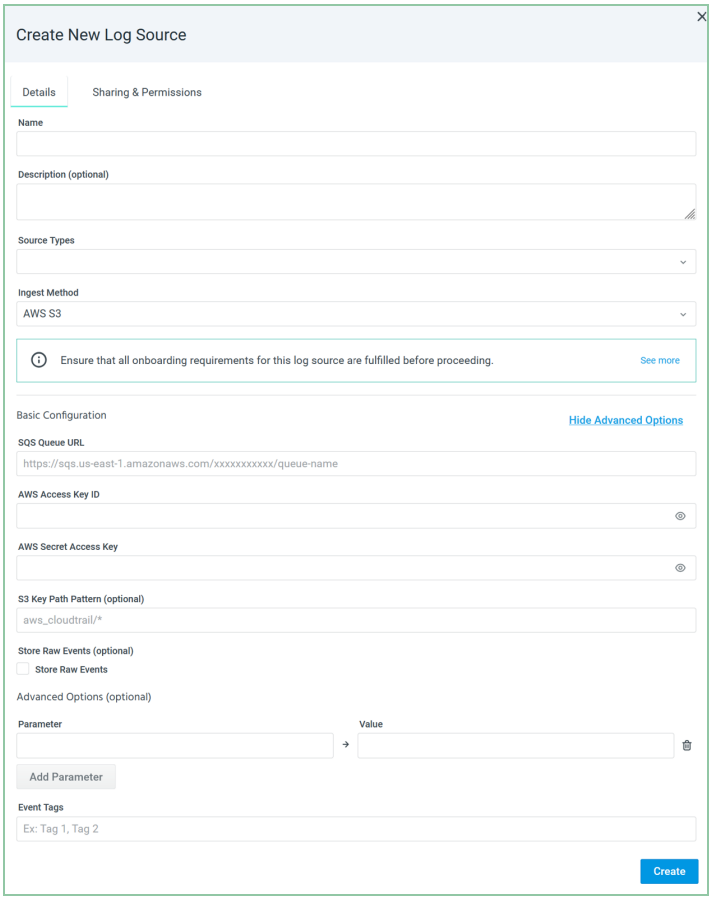
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add F5 BIG-IP TCL Error as new log source



On the Anomali platform, add F5 BIG-IP as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `f5_big_ip_tcl_error/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"f5_big_ip_tcl_error"` is correct, however `"f5 big ip tcl error"` is incorrect.

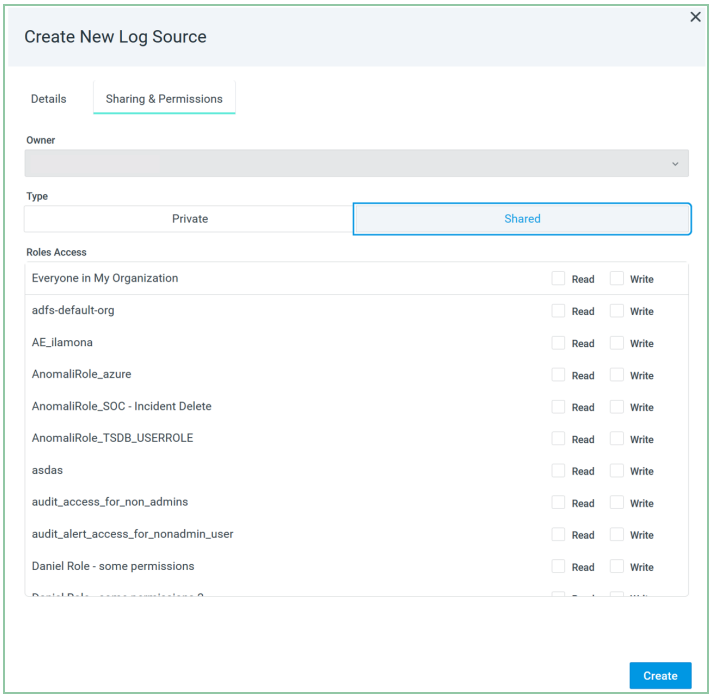
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Forcepoint

Anomali supports the ingestion of Forcepoint logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

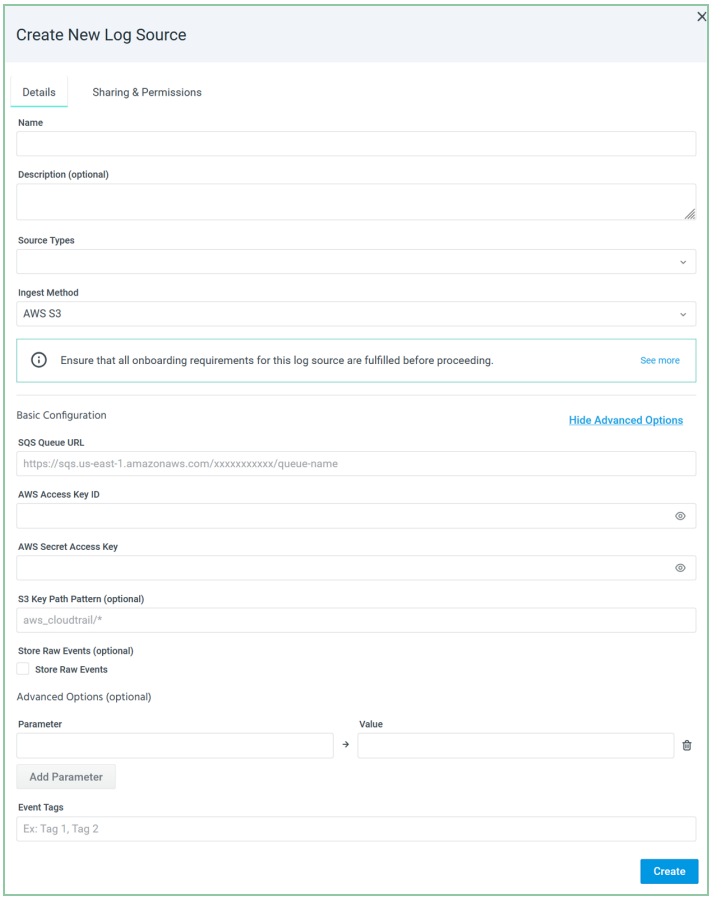
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Forcepoint as new log source



On the Anomali platform, add Forcepoint as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `forcepoint/year=2025/month=03/day=22/events/event_data_logs/`.

- Sourcetype name must not contain any spaces: For example, `"forcepoint"` or `forcepoint_sourcetype` are correct, however `"forcepoint sourcetype"` is incorrect.

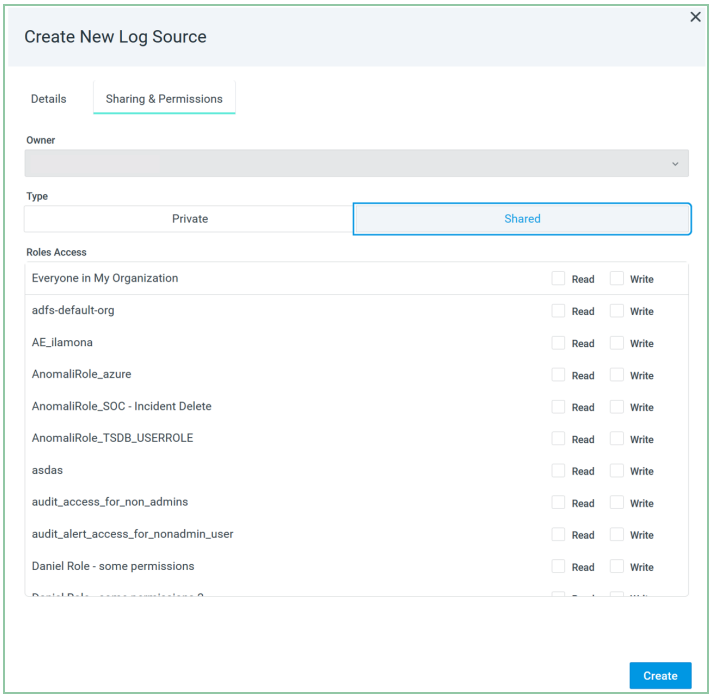
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Fortinet

Anomali supports the ingestion of Fortinet logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

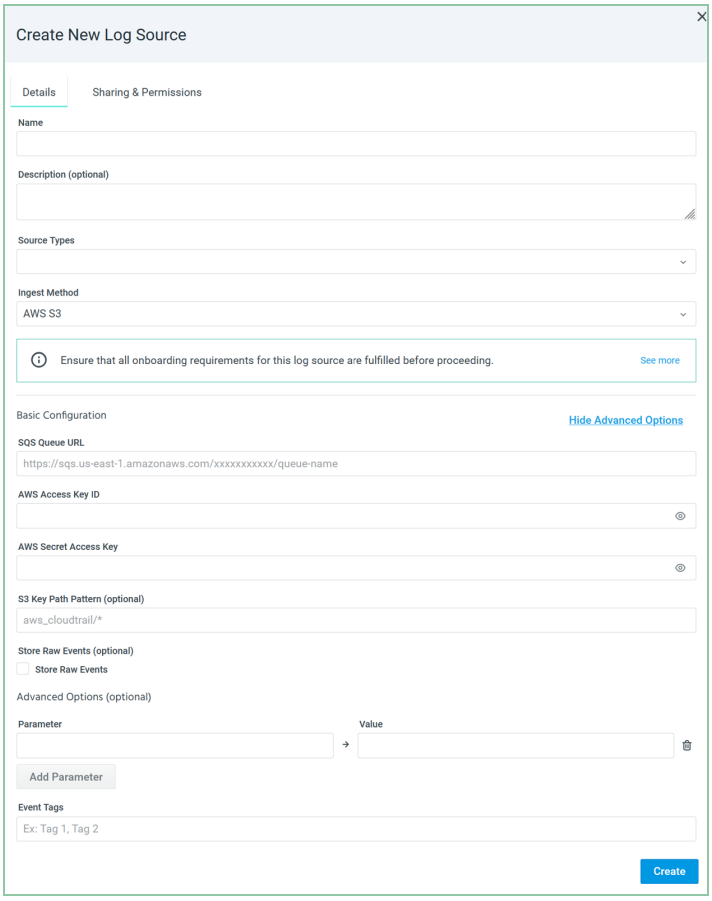
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Fortinet as new log source



On the Anomali platform, add Fortinet as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `fortinet/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"fortinet_sourcetype"` is correct, however `"fortinet sourcetype"` is incorrect.

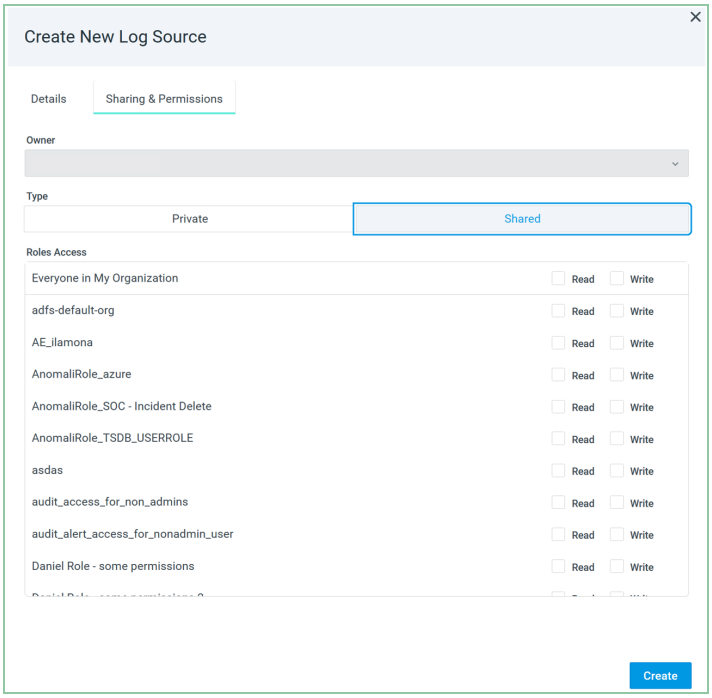
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Google Cloud Platform

Anomali Security Analytics can ingest Google Cloud Platform (GCP) Firewall, GCP VPC, and any other GCP log data. The following article explains the steps you must complete to ingest GCP logs into Anomali.

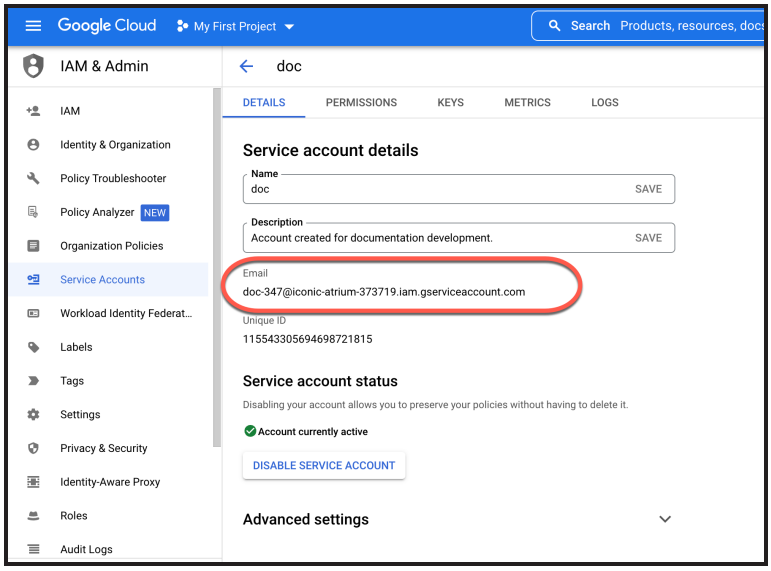
Google Service Account

Step 1: Set Up GCP Resources

1. Create a Google Cloud project. See Google's guide to Creating and managing projects for more information.
2. Create an IAM service account to be used with the project. See Google's guide to Creating and managing service accounts for more information.
3. Within the service account configuration:
   - On the **Keys** tab, generate a service account key file in JSON format. See Google's guide to Create and manage service account keys for more information.

     The key file is downloaded automatically as soon as you generate it. Securely save the key for Step 2: Add GCP as a new log source. Anomali will use the service account key file to authenticate its requests to Google Cloud Storage.
   - On the **Details** tab, copy the email address associated with the service account, so that you can paste it when you set up service account access to

the Google Cloud Storage bucket.

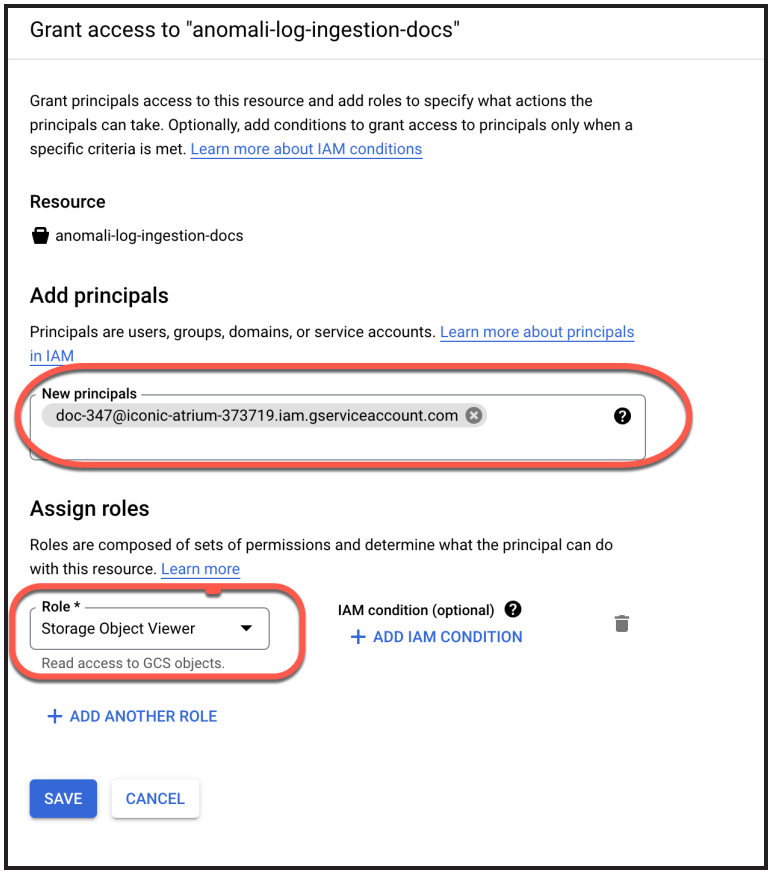


4. Create a Google Cloud Storage Bucket to be used within the project. See Google's guide to Create buckets for more information.

   Within the bucket configuration:

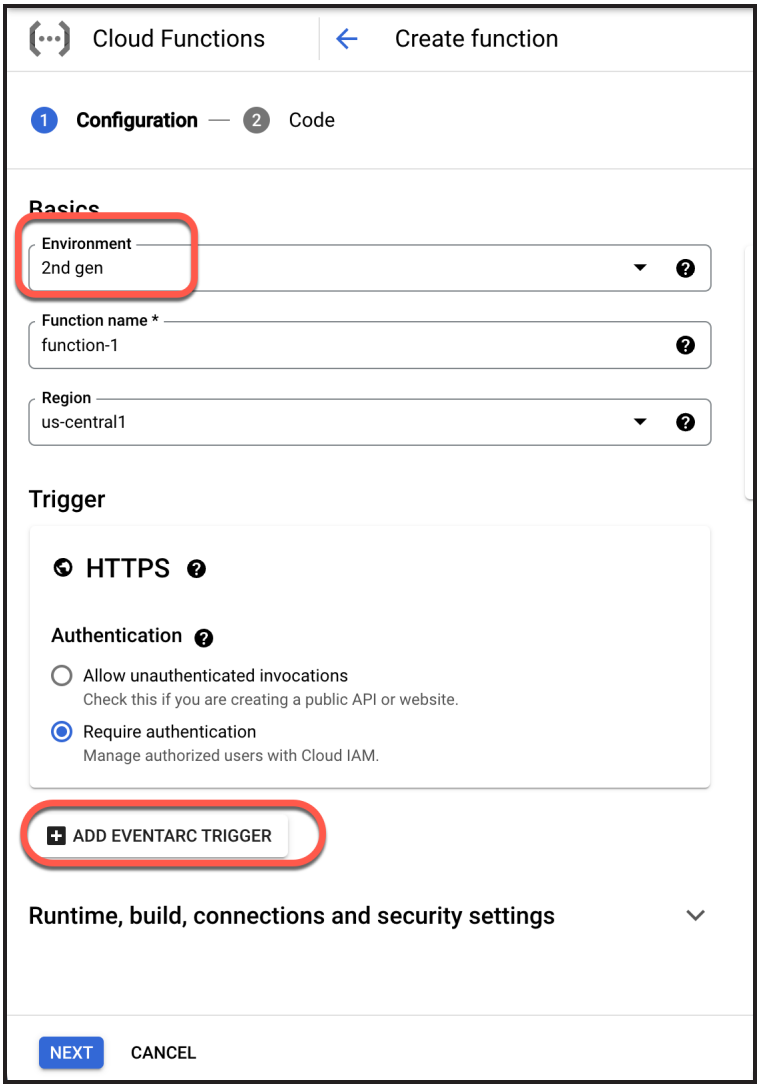
   - Select **Edit access** and click **Add Principal** to display a form you can use to grant access to the service account. See Google's guide to Use IAM with buckets for more information.
   - In the New principals field, paste the service account and select it.

- Select **Storage Object Viewer** as the role.

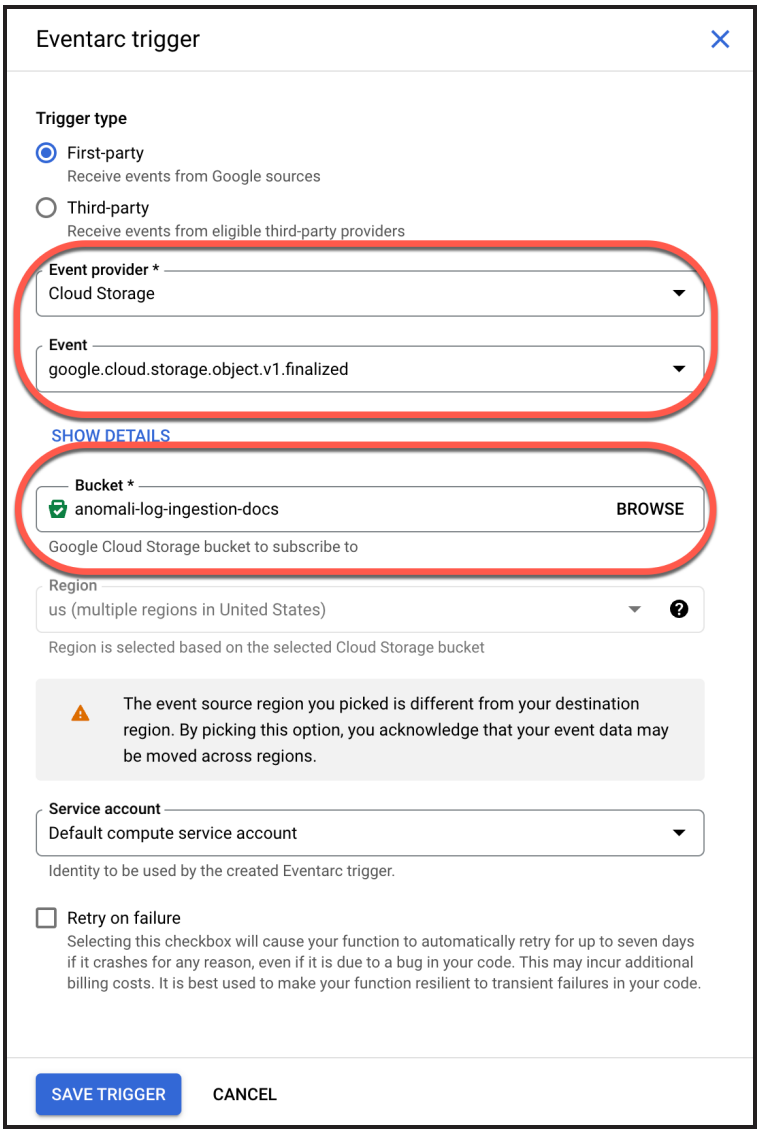


5. Create a Cloud Function, as follows: See Google's guide to Cloud Functions triggers for more information.

a. Select **2nd gen** environment and click **Add Eventarc Trigger**.

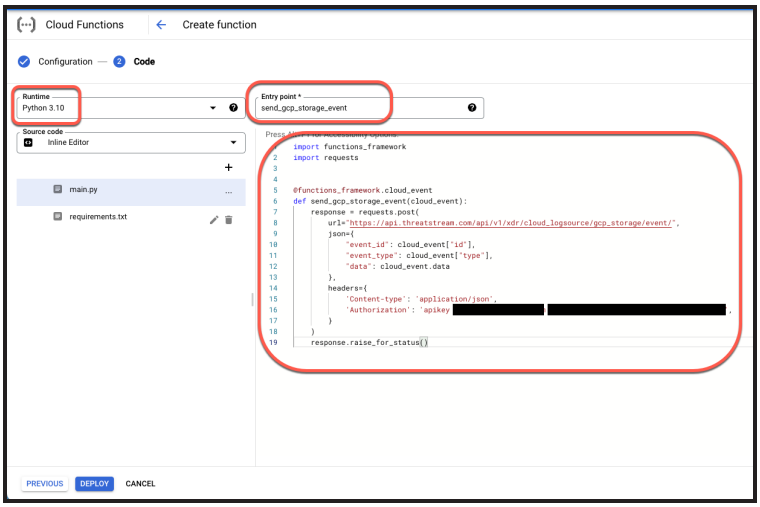


b. Select **Cloud Storage** as the event provider. Select **google.cloud.storage.object.v1.finalized** as the event, and select the storage bucket from "Step 1: Set Up GCP Resources" on page 692. You can use the **Default compute service account** for the Eventarc trigger.



c. Click **Save Trigger**.

d. Edit the function code, as follows:



e. Paste the following code into the function:

```
import functions_framework
import requests

@functions_framework.cloud_event
def send_gcp_storage_event(cloud_event):
    response = requests.post(
        url="https://api.threatstream.com/api/v1/xdr/cloud_
logsource/gcp_storage/event/",
        json={
            "event_id": cloud_event["id"],
            "event_type": cloud_event["type"],
            "data": cloud_event.data
        },
        headers={
            'Content-type': 'application/json',
            'Authorization': 'apikey <email>:<api_key>',
        }
    )
    response.raise_for_status()
```

f. Replace the values for the Authorization API key with the email address and API key for the Anomali service account.

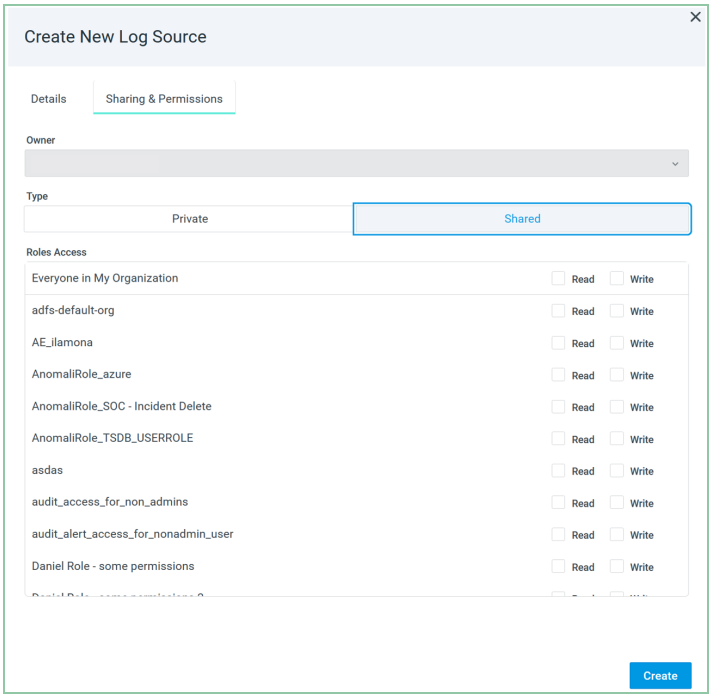
6. Route logs to the Google Cloud Storage bucket. See Google's guide to Route Logs to Supported Destinations for more information.

Step 2: Add GCP Firewall or VPC or Auto as new log source

To add GCP Firewall or VPC as a new log source on the Anomali platform:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select **GCP Firewall** or **GCP VPC** or **GCP Auto** as the source type.
6. Select **API** as the ingestion method.
7. Select API as the ingest method.
8. Provide the Basic Configuration details:
   a. **Google User**: Enter the provisioned storage account name. Refer to "Step 1: Set Up GCP Resources" on page 692.
   b. **GCP Service Account Credentials**: Click **Browse** and then locate, select, and upload the key file that contains the GCP service account credentials. Refer to"Step 1: Set Up GCP Resources" on page 692.
   c. **GCP Storage Bucket Name**: Enter the bucket name from "Step 1: Set Up GCP Resources" on page 692.
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:
   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.
   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.
10. Click **Save** to add the log source.

Step 3: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 4: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 5: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

AWS S3

If your logs are already in S3, you can proceed directly to "Step 2: Add GCP Firewall or VPC or Auto as new log source" on page 698. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

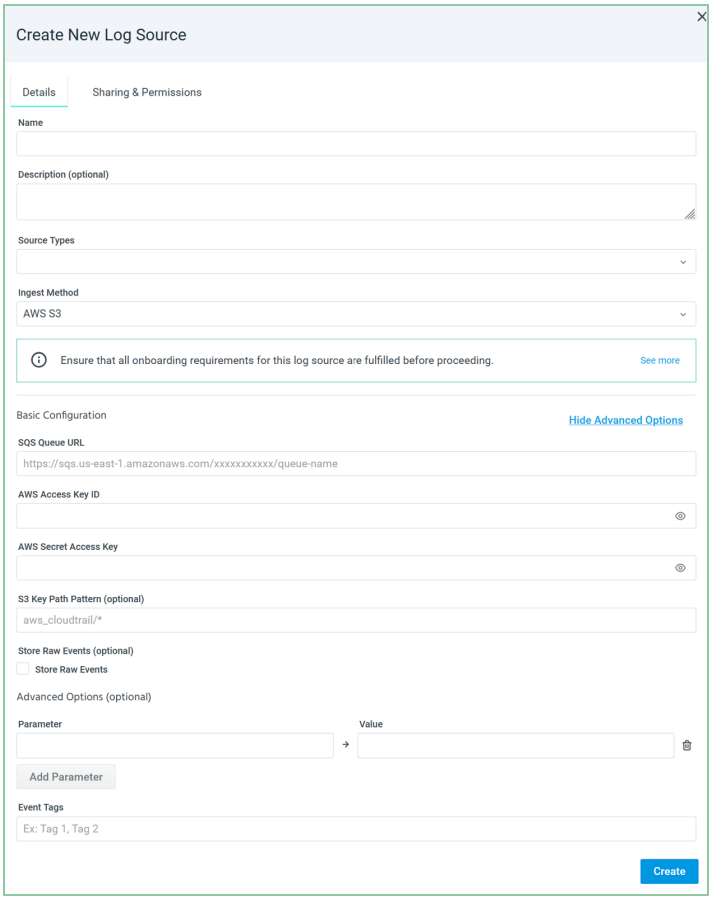
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add GCP VPC or Firewall or Auto as new log source



On the Anomali platform, add GCP VPC or Firewall or Auto as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.

8. Provide the Basic Configuration details:

   a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

   b. **AWS Secret Access Key**: Provide the AWS secret access key.

   c. **AWS Access Key ID**: Enter the AWS Access ID.

   d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

   - Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `gcp_vpc/year=2025/month=03/day=22/events/event_data_logs/`.

   - Sourcetype name must not contain any spaces: For example, `"gcp_vpc"` or `"gcp_firewall"` are correct, however `"gcp firewall"` is incorrect.

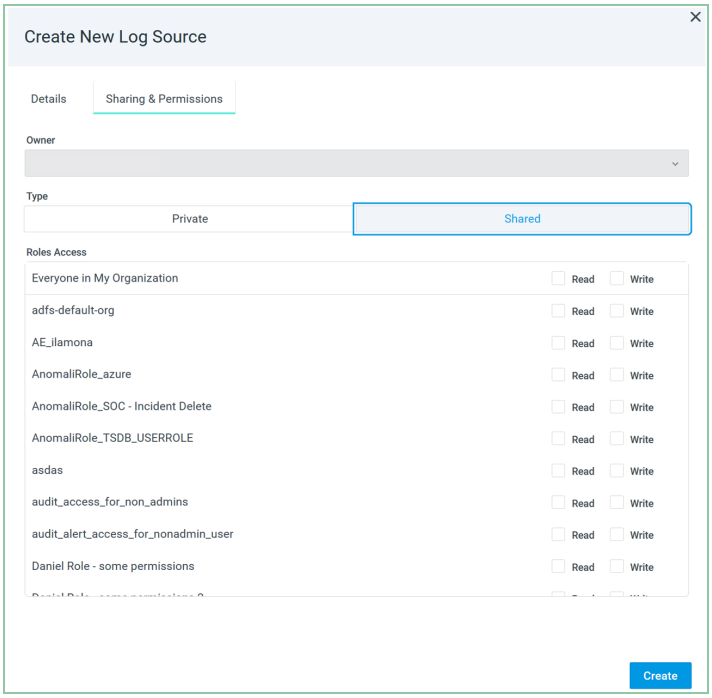
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Google SecOps

This document explains how you can configure Google SecOps to send alerts to Anomali using the Google SecOps API, and add Google SecOps as a log source in the Anomali platform.

Specifically, this configuration enables Anomali to periodically pull the following alerts from Google SecOps for enrichment, correlation, and downstream intelligence workflows:

- Curated alerts: These are alerts produced by out-of-the-box detection rules that are authored, maintained, and updated by Google.
- Custom alerts: These are alerts produced by rules you create inside Google SecOps.

Google SecOps API

You can use your existing Google Cloud service account or create a new service account to add a new log source in the Anomali platform.

Onboarding steps

Prerequisites

Before adding Google SecOps as a log source, you must fulfill the following prerequisites:-

Google SecOps prerequisites

- An active Google SecOps tenant.
- Permissions to:
  - Create or access a service account
  - Download service account credentials (in JSON format)

  - Read alerts via the Google SecOps API
- Access to your:
  - Project ID
  - Instance ID (Customer ID)
  - Deployment location (region)

Regional Endpoints

Google SecOps APIs are region-specific. Select the endpoint that corresponds to your SecOps deployment region.

See Google SecOps Regional Endpoint documentation for more information.

Step 1: Download Google SecOps Service Account Credentials

In the Google SecOps platform:

1. Create or select a service account with alert read permissions.
2. Generate and download the service account key in JSON format.

Step 2: Retrieve Google SecOps Identifiers

From Google SecOps, retrieve the following identifiers:-

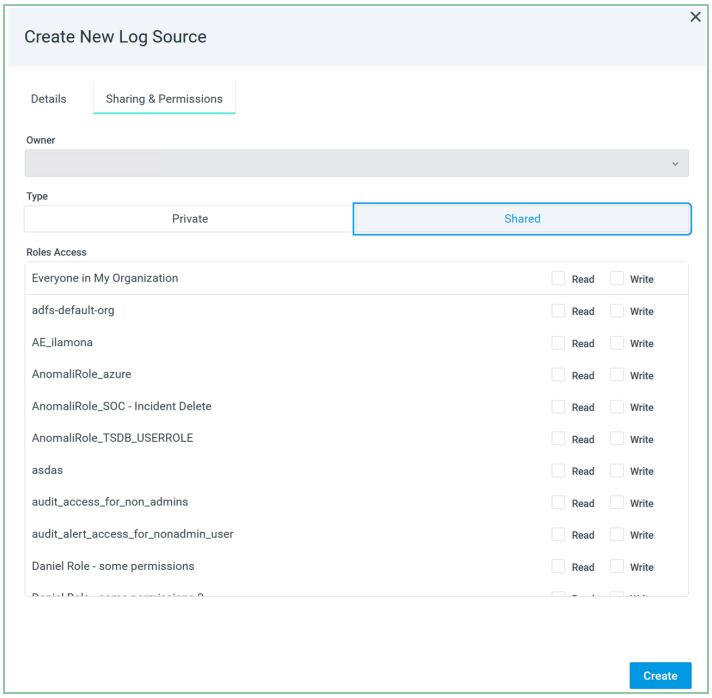
Field	Description
Project ID	Google Cloud project associated with SecOps.
Instance ID	This is also the Customer ID.
Location	Region where SecOps is deployed.
Regional endpoint	API endpoint corresponding to the region.

Step 3: Add Google SecOps as new log source

To add Google SecOps as a new log source on the Anomali platform and allow Anomali to correctly scope and authenticate API requests:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the source type.
5. Select **Google SecOps** as the log source.
6. Select **API** as the ingestion method.
7. Provide the Basic Configuration details:
   a. **Regional Endpoint URL**: Enter the regional endpoint URL from "Step 2: Retrieve Google SecOps Identifiers" on the previous page.
   b. **Project ID**: Enter the Project ID from "Step 2: Retrieve Google SecOps Identifiers" on the previous page.
   c. **Location**: Enter the deployment region from "Step 2: Retrieve Google SecOps Identifiers" on the previous page.
   d. **Service Account Credentials**: Enter the service account credentials from "Step 1: Download Google SecOps Service Account Credentials" on the previous page.
   e. **Instance ID**: Enter the Instance ID from "Step 2: Retrieve Google SecOps Identifiers" on the previous page.
8. (Optional) Click **Show Advanced Options** to:
   a. Enable custom alerts or curated alerts and send custom or curated alerts to Anomali.
   b. Set the ingestion interval value in minute, hour, or day. The default value is 10 minutes.
9. Click **Save** to add the log source.

Step 4: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 5: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 6: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Google Workspace

Anomali supports the ingestion of Google Workspace logs through the Google Workspace Reports API and AWS S3.

Google Workspace API

You can use your existing Google Cloud service account or create a new service account to add a new log source in the Anomali platform.

Onboarding steps

Prerequisites

Your Google user must be authorized to read your organization's activity records. If your user does not have this privilege, follow Google Workspace instructions to create a new role with Reports access and assign the role to your user.

Step 1: Create Google Cloud Project

See Google's guide to Creating and managing projects to learn how you can create a Google Cloud project.

Step 2: Create service account

See Google's guide to Creating a service account.

Step 3: Enable Workspace Admin SDK API

Google Workspace Admin SDK API contains the following APIs:

- Google Workspace Reports API
- Google Workspace Alert Center API

To enable these APIs:

1. Navigate to the APIs Library and select **APIs and Services** > **Library**.
2. Search for `Admin SDK API` and select Admin SDK API.
3. Click **Enable** to enable the Admin SDK API.
4. Similarly, search for `Alert Center API` and click **Enable** to enable the Alert Center API.

Step 4: Create API credentials

1. Navigate to **API Credentials** > **APIs and Services** > **Credentials**.
2. Click **Create Credentials** > **Service Account**.
3. Enter a service account name. This also populates a service account ID.
4. (Optional) Enter a service account description.
5. Click **Done**.
6. From the Service Accounts table, select the service account that was created.
7. Securely save the Unique ID value displayed. This ID will be necessary for "Google Workspace " on the previous page.
8. From the Keys menu, click **Add Key** > **Create new key**.
9. Select JSON as the key type.
10. Click **Create**. This saves a JSON file to your local filesystem containing the secure access credentials for this service acount.

Step 5: Delegate domain-wide authority

1. Log in to the Google Admin Console.
2. Navigate to **API Controls** > **Security** > **Access and data control** > **API controls**.
3. Click **Manage Domain Wide Delegation**.
4. Click **Add new**.
5. In the Client ID field, enter the Unique ID from "Google Workspace " on the previous page.
6. In the OAuth scopes, enter the following:
7. Click **Authorize**.

Step 6: Create new role for new or existing user

1. Log in to the Google Admin Console.
2. Click **Create New Role**.
3. Enter a Name and Description for the role info, then click **Continue**.
4. From the Services section, select the **Reports** privilege. Additionally, in the Alert Center section, select **View access** privilege.
5. Click **Continue**.
6. Click **Create Role**.
7. Then, either add a user by clicking **Add new user** or use an existing user. This page includes the primary email address for the user to sign in.
8. Click **Assign roles** from Admin roles and privileges.
9. Select the role you created and toggle the Assigned state switch to assign the role.
10. Click **Save**.

Securely save the email address of this user for "Google Workspace " on page 709.

Step 7: Add Google Workspace as new log source

To add Google Workspace as a new log source on the Anomali platform:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the source type.
5. Select **Google Workspace** as the log source.
6. Select **API** as the ingestion method.
7. Provide the Basic Configuration details:

a. **Google User**: Enter the email address of the Google Workspace user from "Google Workspace " on page 709.

b. **GCP Service Account Credentials**: Enter the password of the Google service account.

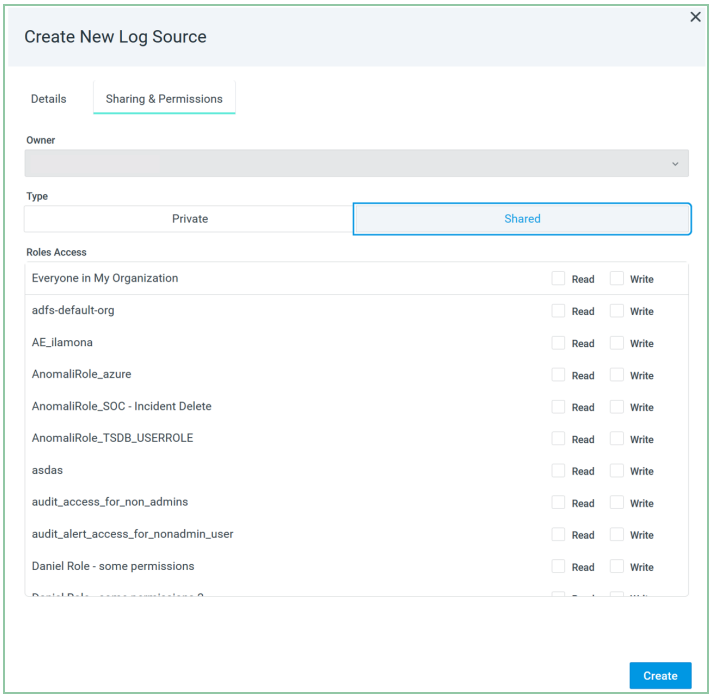
8. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

9. Click **Save** to add the log source.

Step 8: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 9: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 10: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

AWS S3

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

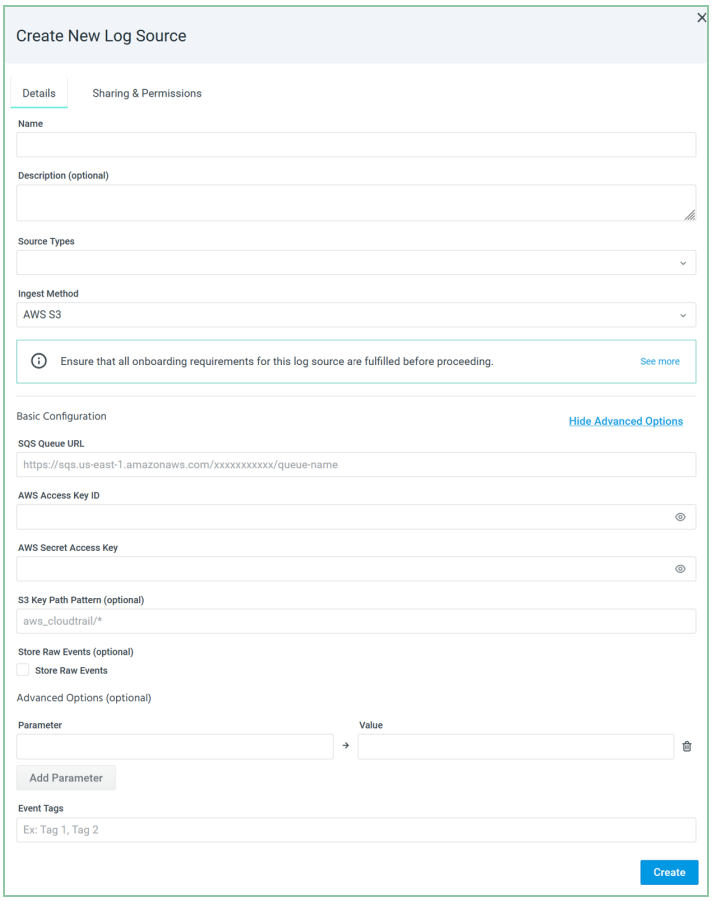
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Google Workspace as new log source

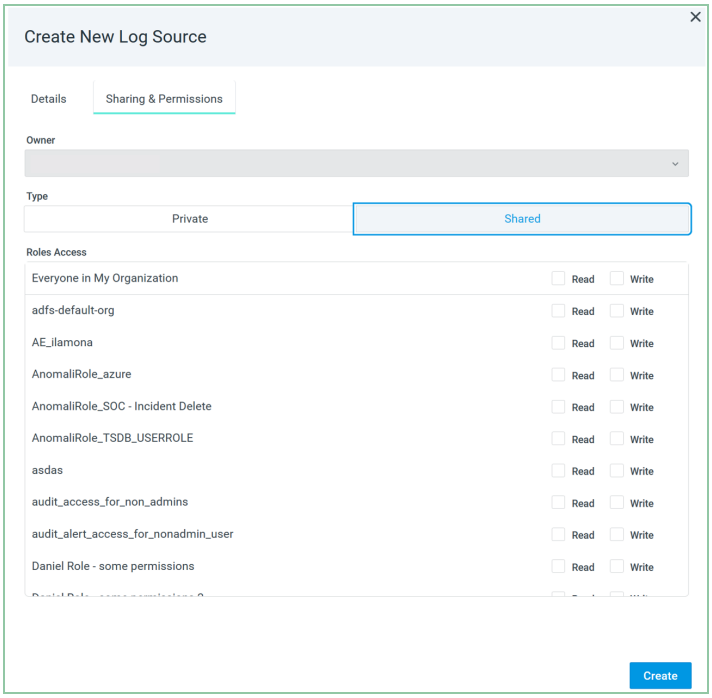


On the Anomali platform, add Google Workspace as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.

5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:
   a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.
   b. **AWS Secret Access Key**: Provide the AWS secret access key.
   c. **AWS Access Key ID**: Enter the AWS Access ID.
   d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:
      - Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `google_workspace/year=2025/month=03/day=22/events/event_data_logs/`.
      - Sourcetype name must not contain any spaces: For example, `"google_workspace"` is correct, however `"google workspace"` is incorrect.
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:
   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.
   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.
10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

GitHub Cloud

Anomali supports the ingestion of GitHub Cloud logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

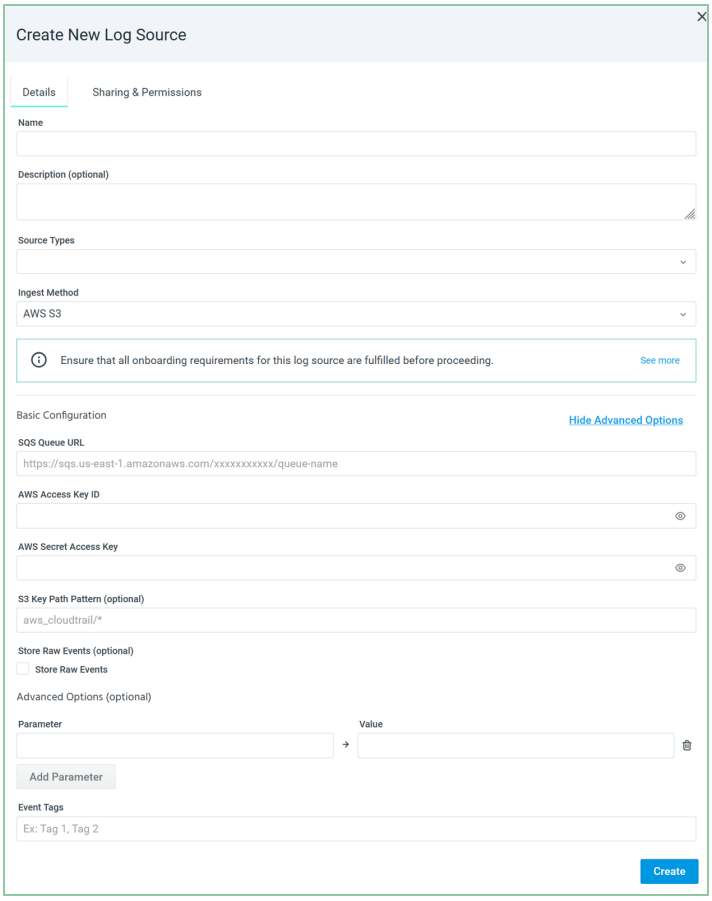
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add GitHub Cloud as new log source



On the Anomali platform, add GitHub Cloud as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `github_cloud/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"github_cloud"` is correct, however `"github cloud"` is incorrect.

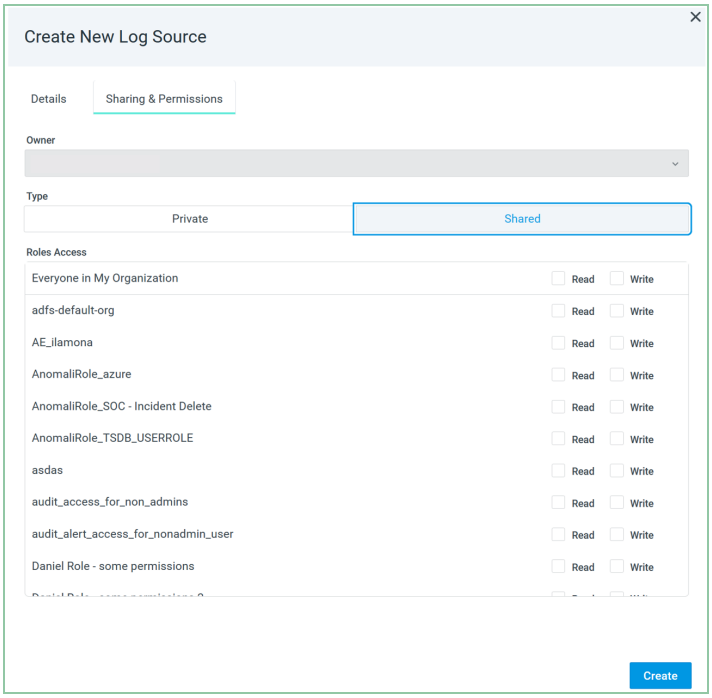
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Guardicore Centra

Anomali supports the ingestion of Guardicore Centra logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

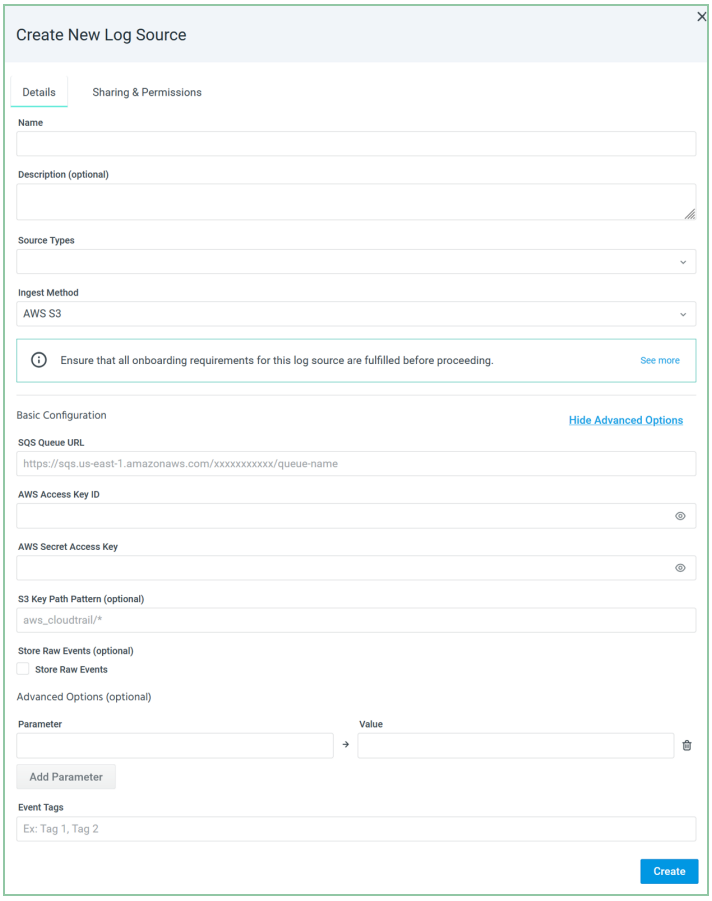
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Guardicore Centra as new log source



On the Anomali platform, add Guardicore Centra as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `guardicore_centra/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"Guardicore_Centra"` is correct, however `"Guardicore Centra"` is incorrect.

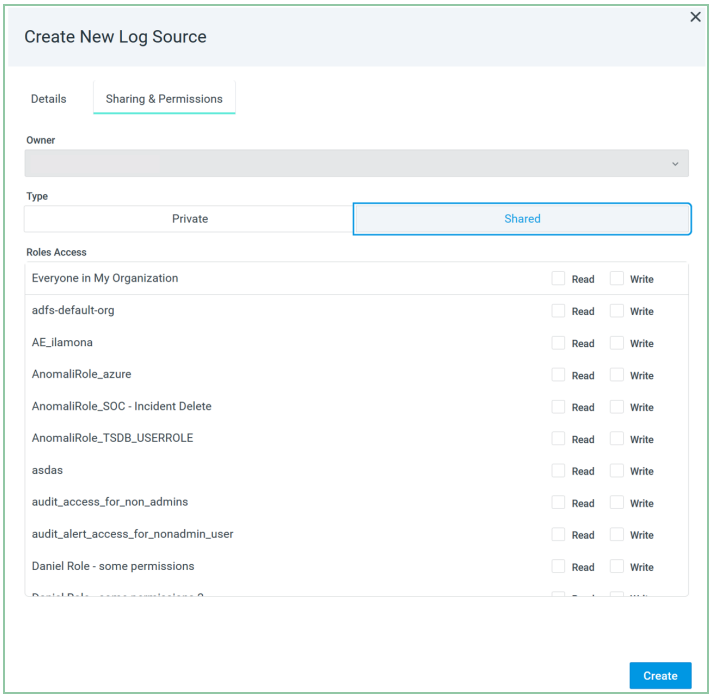
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

HA Proxy

Anomali supports the ingestion of High Availability Proxy logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

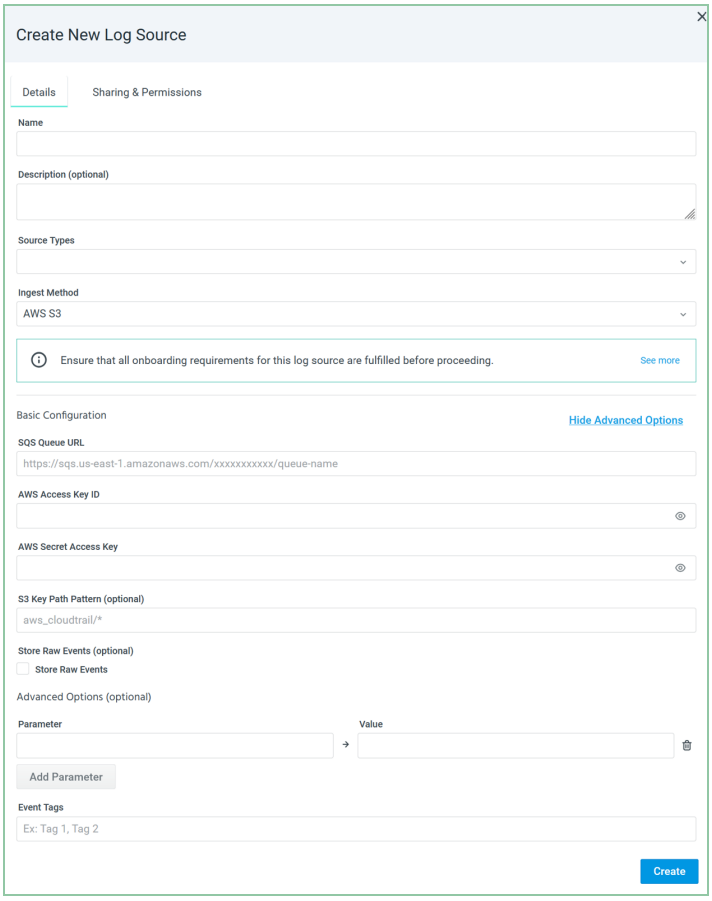
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add HA Proxy as new log source



On the Anomali platform, add HA Proxy as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `ha_proxy/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"ha_proxy"` is correct, however `"ha proxy"` is incorrect.

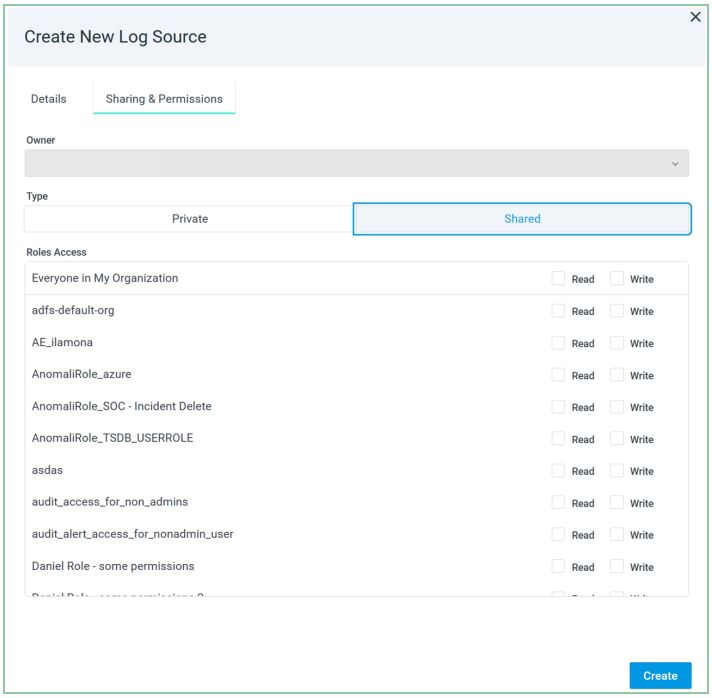
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

IdentityIQ

Anomali supports the ingestion of IdentityIQ logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

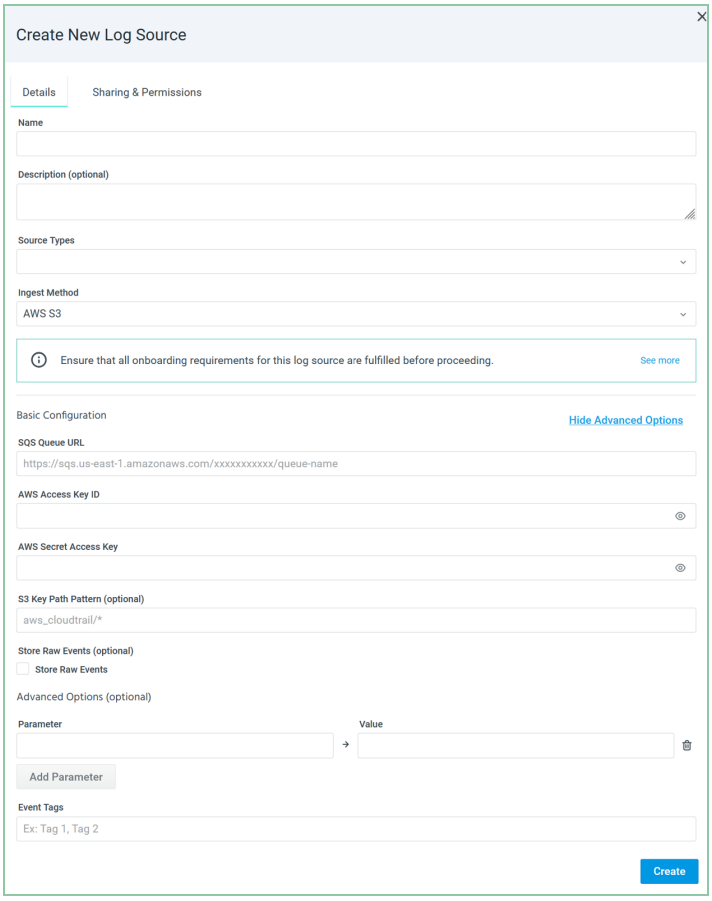
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add IdentityIQ as new log source



On the Anomali platform, add IdentityIQ as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `identityIQ/year=2025/month=03/day=22/events/event_data_logs/`.

- Sourcetype name must not contain any spaces: For example, `"identityIQ"` or `"identityIQ_sourcetype"` are correct, however `"IdentityIQ Sourcetype"` is incorrect.

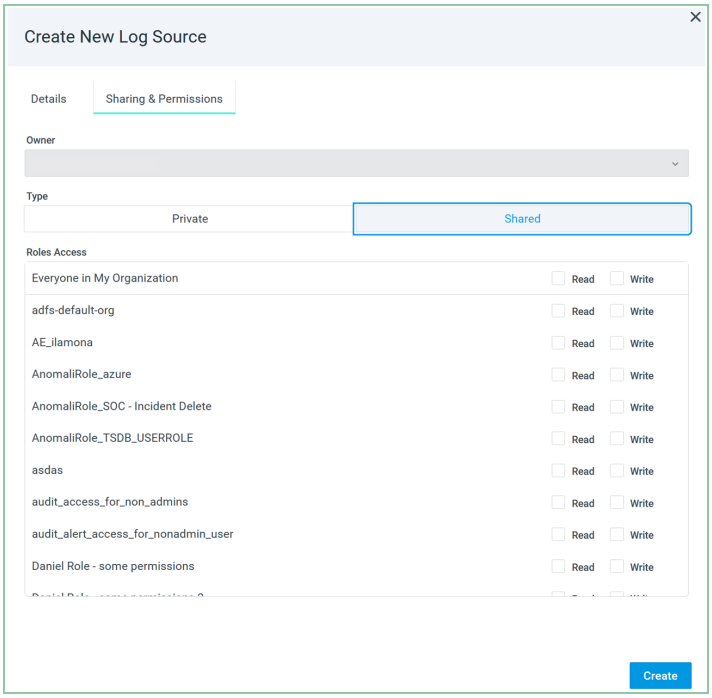
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

IIS

Anomali supports the ingestion of Internet Information Service (IIS) logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

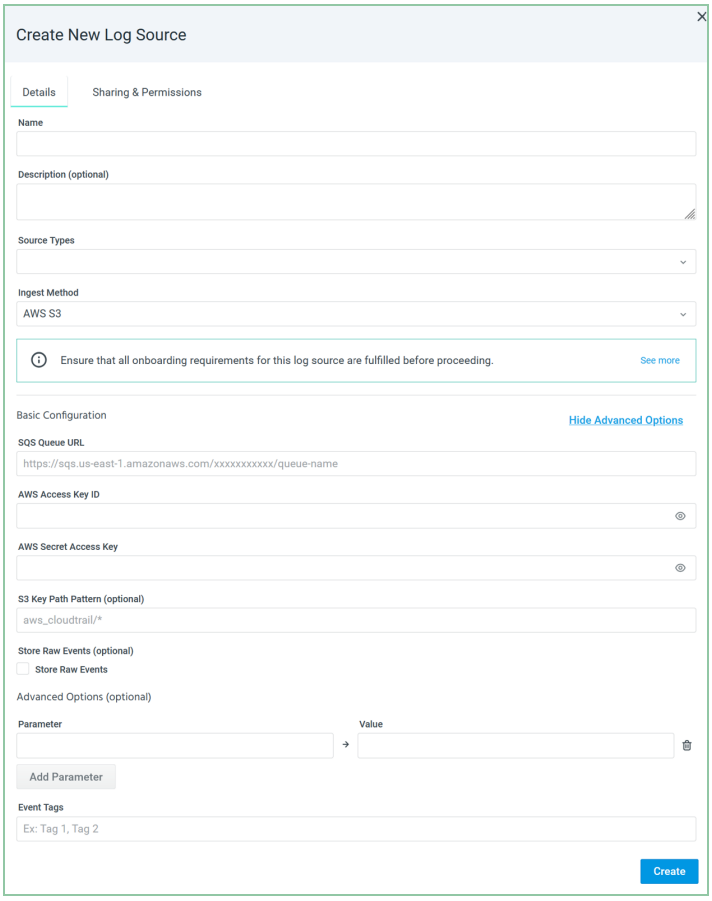
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add IIS as new log source



On the Anomali platform, add IIS as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `iis/year=2025/month=03/day=22/events/event_data_logs/`.

- Sourcetype name must not contain any spaces: For example, `"iis"` or `"iis_sourcetype"` are correct, however `"iis sourcetype"` is incorrect.

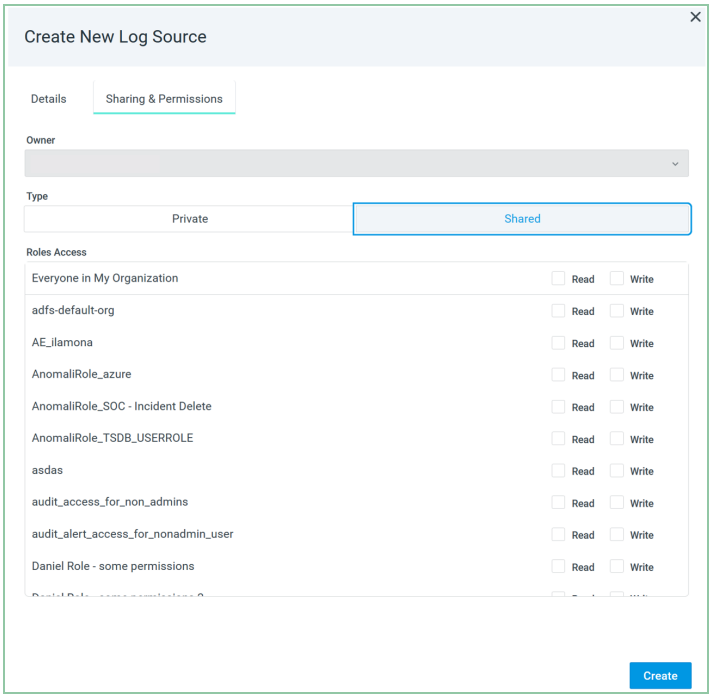
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Infoblox

Anomali supports the ingestion of Infoblox logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

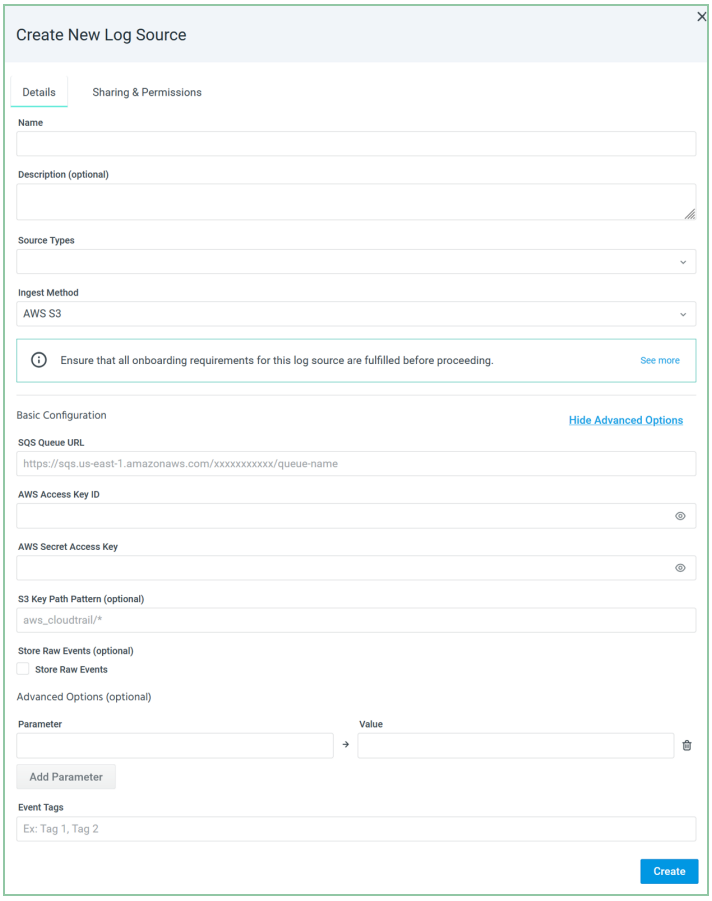
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Infoblox as new log source



On the Anomali platform, add Infoblox as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `infoblox/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"infoblox"` or `"infoblox_sourcetype"` are correct, however `"infoblox sourcetype"` is incorrect.

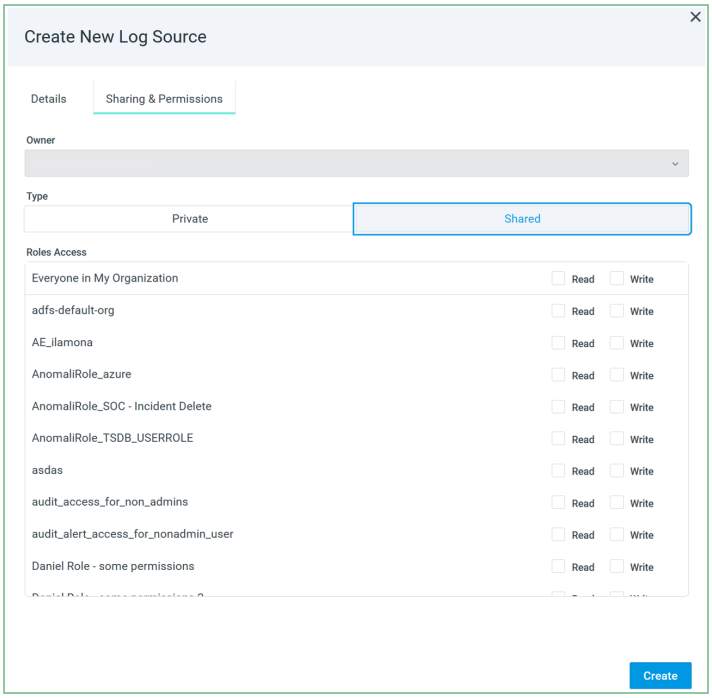
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions

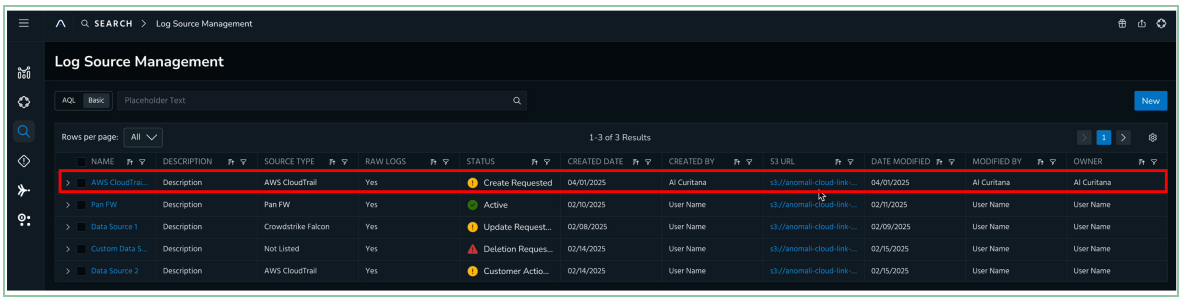


You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.



Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Infoblox Audit

Anomali supports the ingestion of Infoblox Audit logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

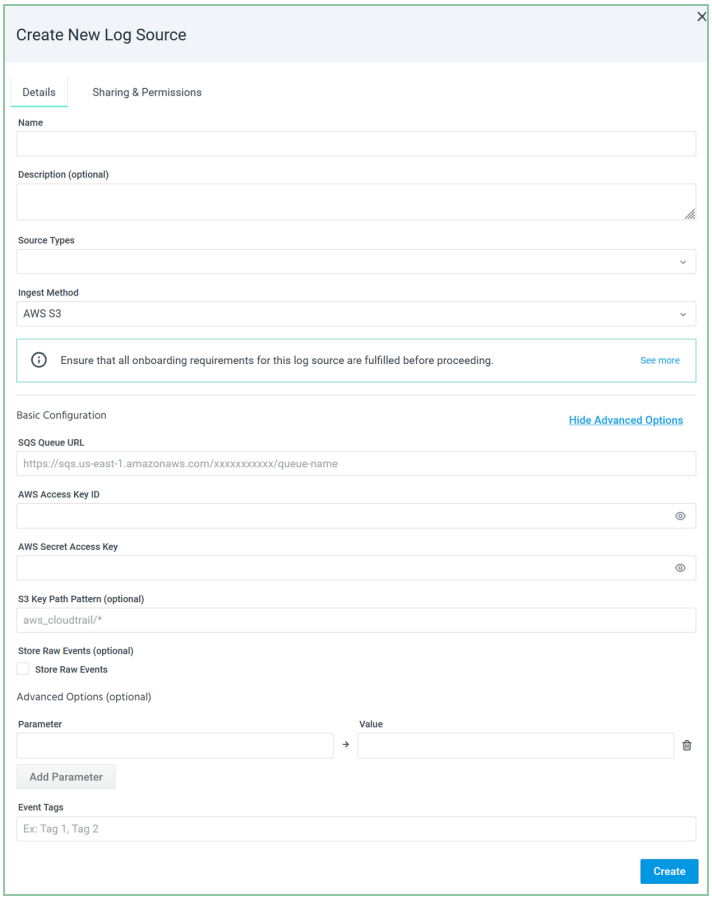
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Infoblox Audit as new log source



On the Anomali platform, add Infoblox Audit as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `infoblox_audit/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"infoblox_audit"` is correct, however `"infoblox audit"` is incorrect.

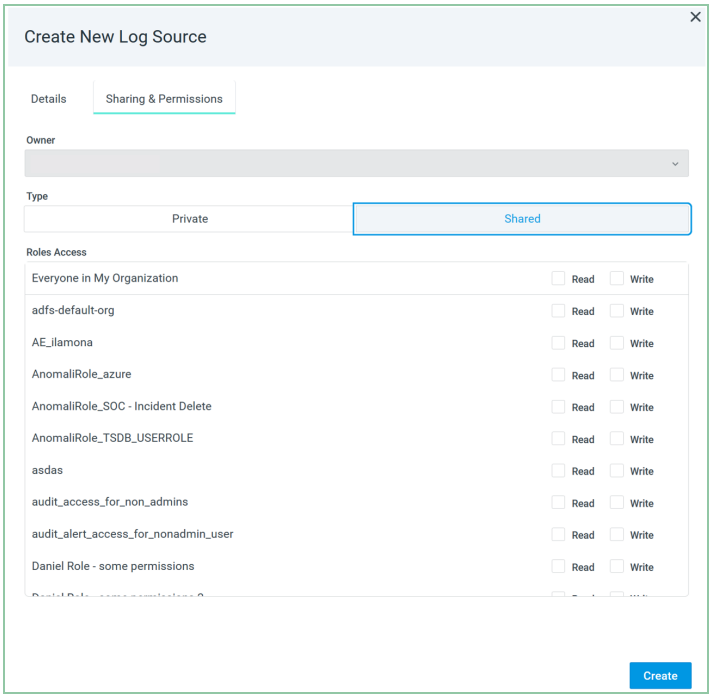
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Infoblox File

Anomali supports the ingestion of Infoblox File logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

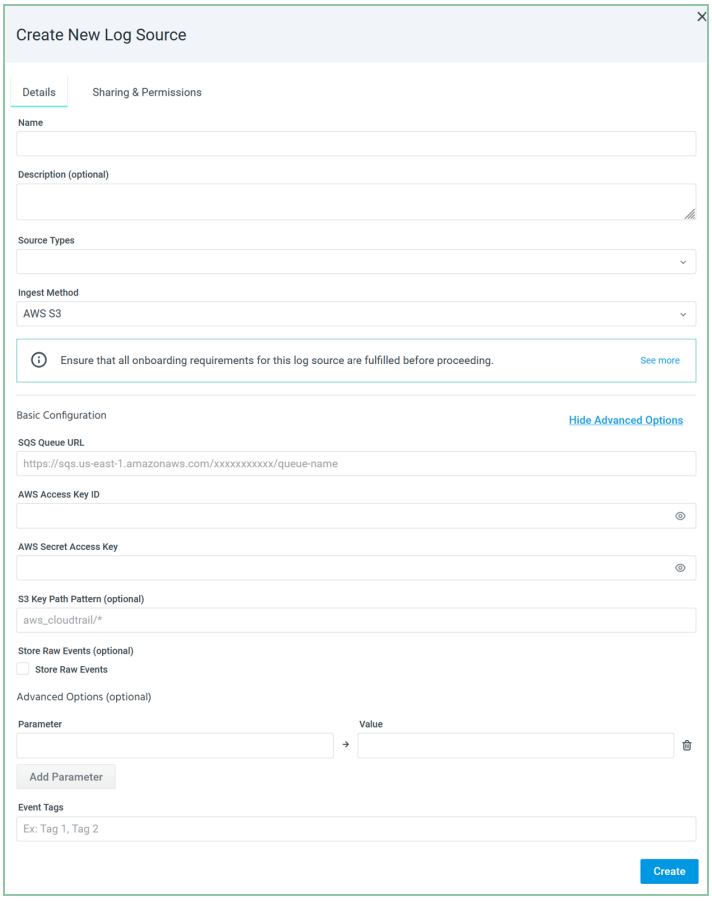
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Infoblox File as new log source



On the Anomali platform, add Infoblox File as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `infoblox_file/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"infoblox_file"` is correct, however `"infoblox file"` is incorrect.

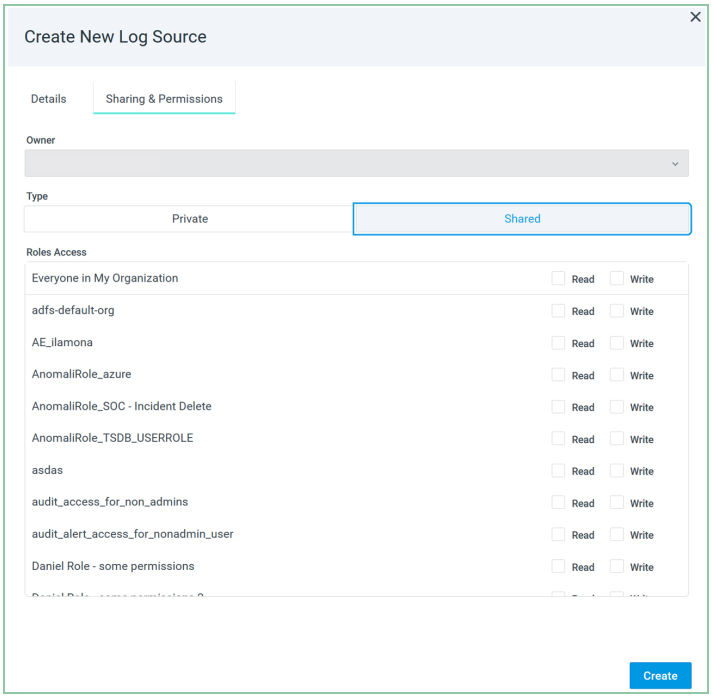
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

JumpCloud

Anomali supports the ingestion of JumpCloud logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

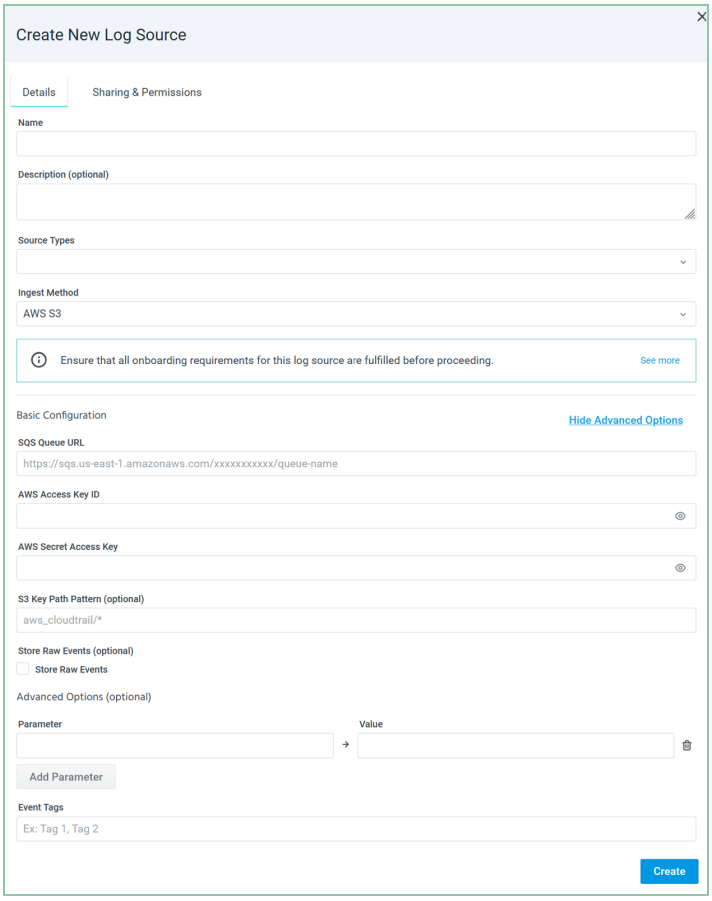
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add JumpCloud as new log source



On the Anomali platform, add JumpCloud as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `jumpcloud/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"jumpcloud_sourcetype"` is correct, however `"jumpcloud sourcetype"` is incorrect.

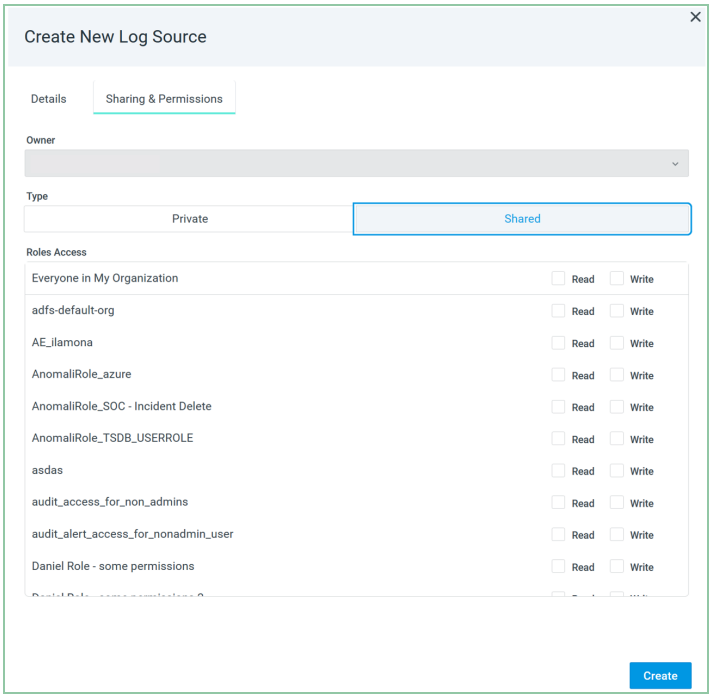
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Juniper Corero

Anomali supports the ingestion of Juniper Corero logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

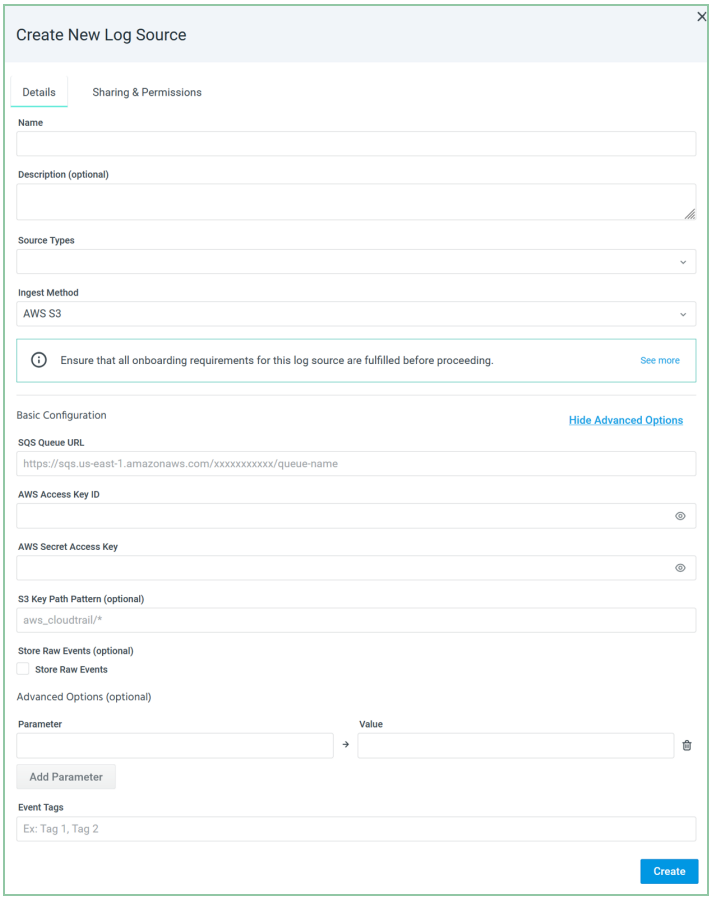
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Juniper Corero as new log source



On the Anomali platform, add Juniper Corero as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `juniper_corero/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"juniper_corero"` is correct, however `"Juniper Corero"` is incorrect.

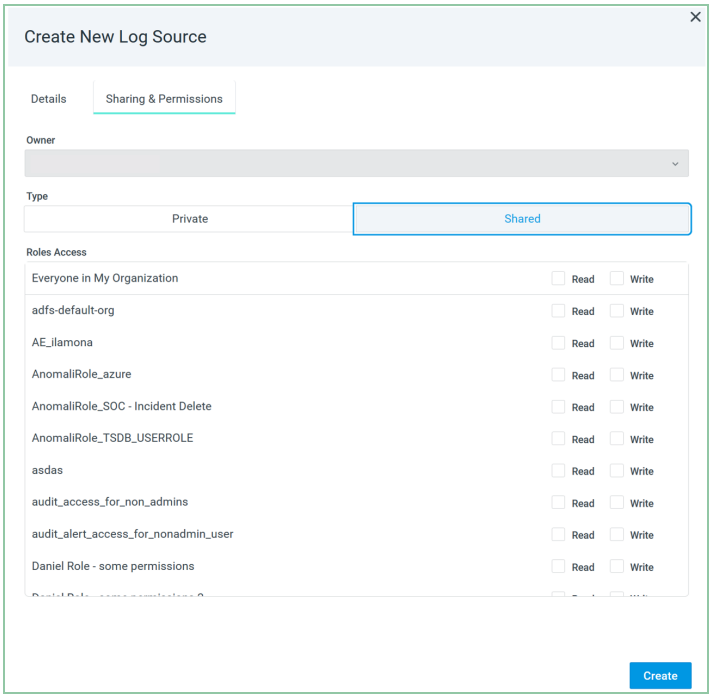
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Juniper JUNOS

Anomali supports the ingestion of Juniper JUNOS logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

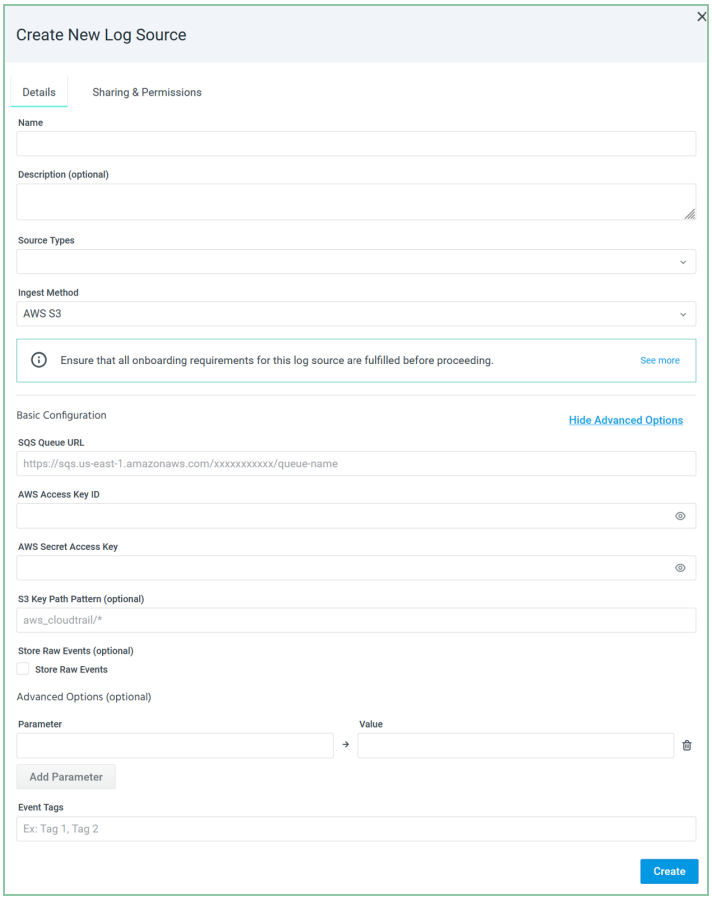
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Juniper as new log source



On the Anomali platform, add Juniper as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `juniper_junos/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"juniper_junos"` is correct, however `"juniper junos"` is incorrect.

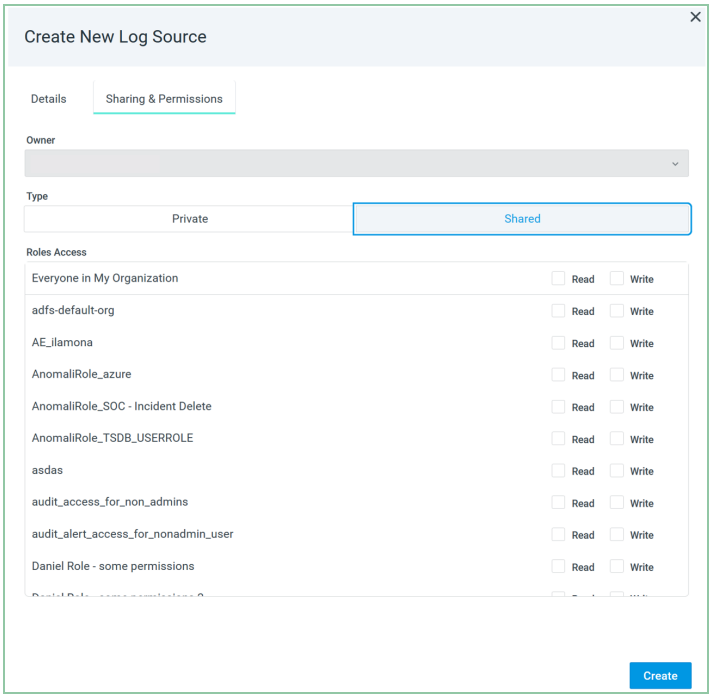
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Juniper Switches

Anomali supports the ingestion of Juniper Switches logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

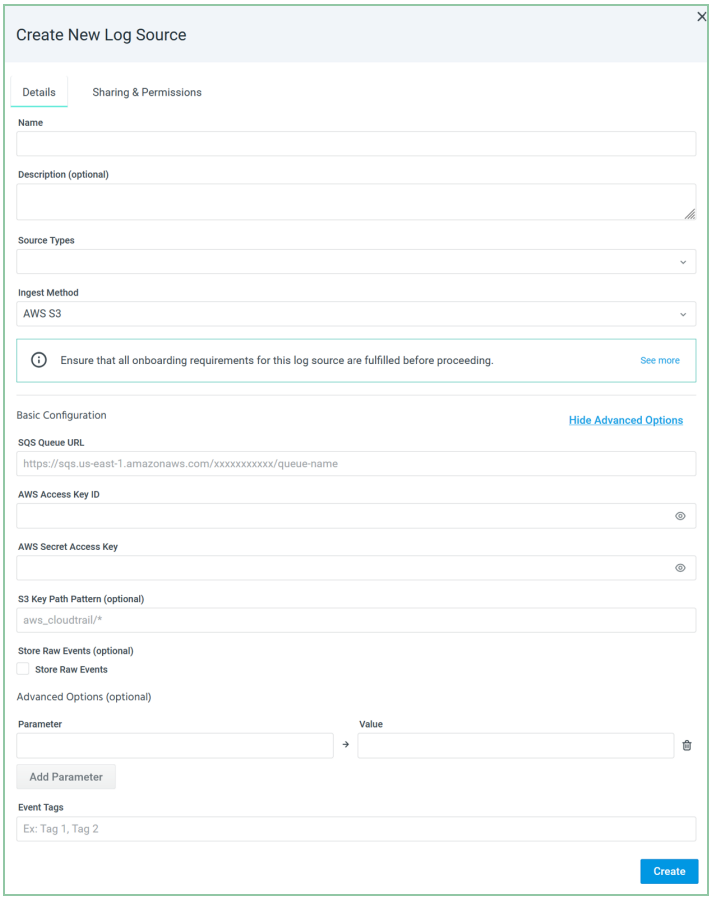
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Juniper Switches as new log source



On the Anomali platform, add Juniper Switches as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `juniper_switches/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"juniper_switches"` is correct, however `"Juniper Switches"` is incorrect.

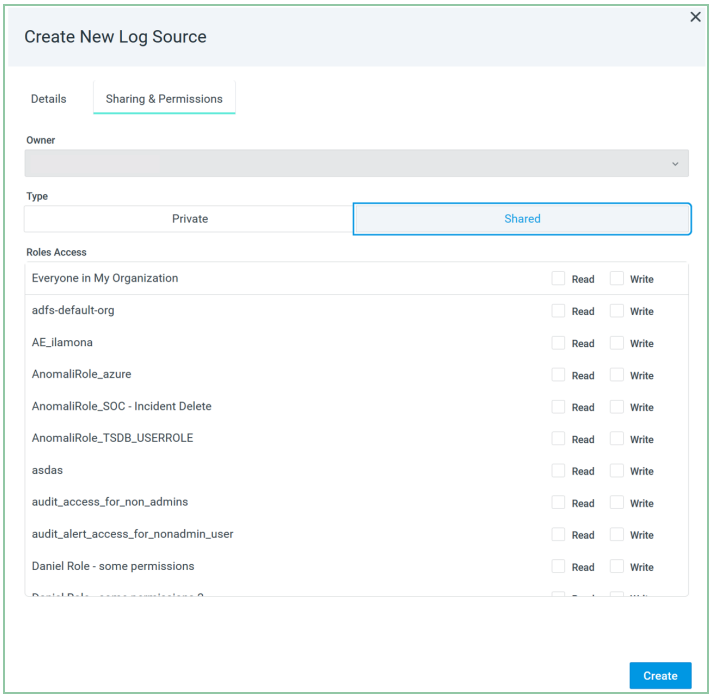
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Linux Audit

Anomali supports the ingestion of Linux Audit logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

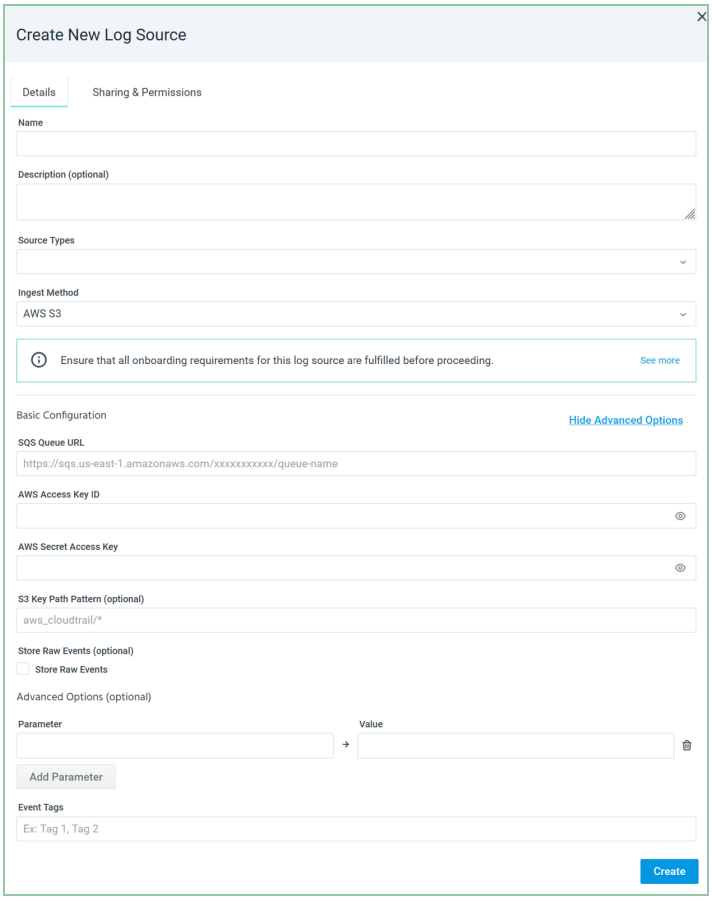
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Linux Audit as new log source



On the Anomali platform, add Linux Audit as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `linux_audit/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"linux_audit"` is correct, however `"linux audit"` is incorrect.

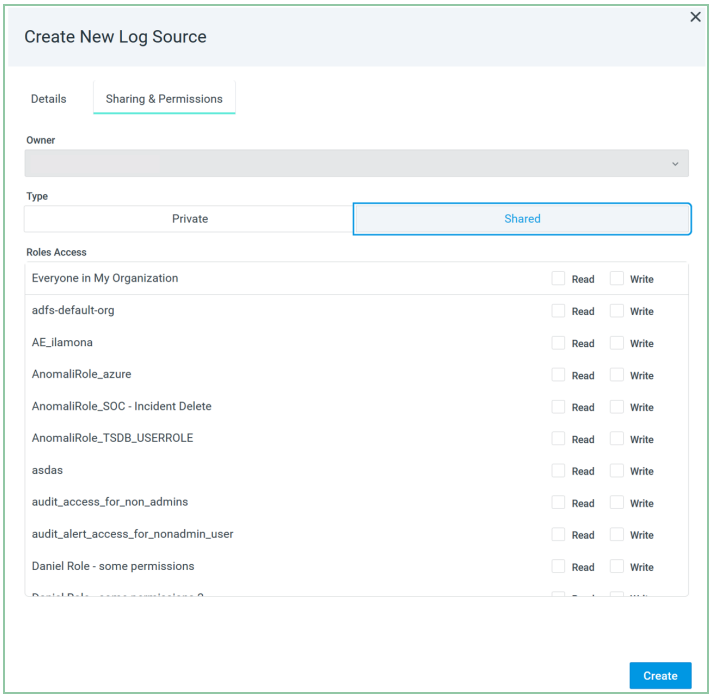
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Linux Auth

Anomali supports the ingestion of Linux Auth logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

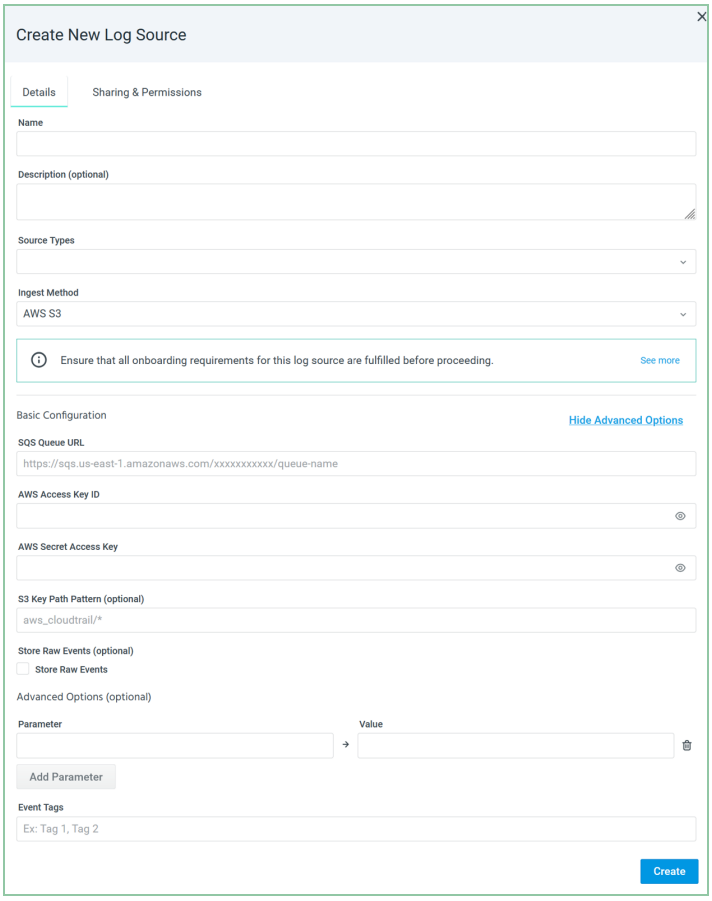
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Linux Auth as new log source



On the Anomali platform, add Linux Auth as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `linux_auth/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"linux_auth"` is correct, however `"linux auth"` is incorrect.

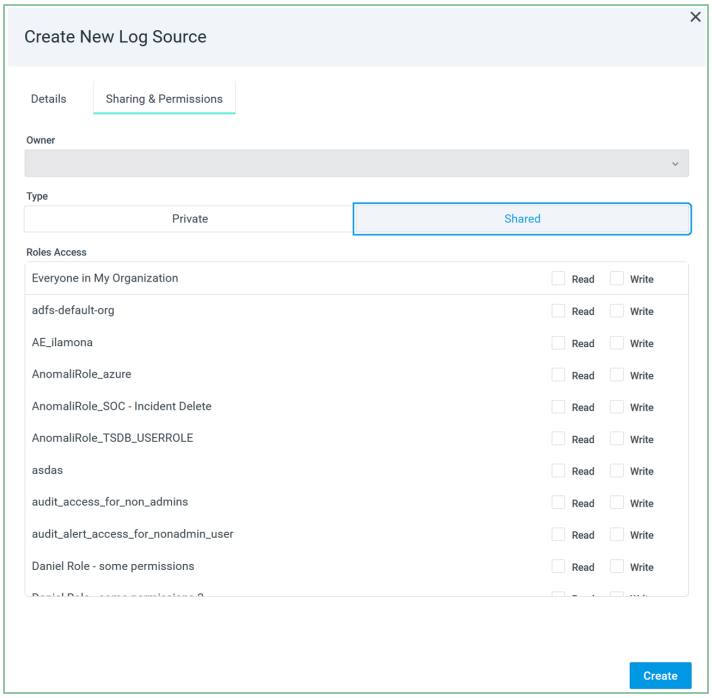
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Mimecast

Anomali supports the ingestion of Mimecast logs through the Mimecast API 2.0 and AWS S3.

Version 2.0 API call

You can use your existing Mimecast Client ID and Client Secret or create them to add a new log source in the Anomali platform.

Onboarding steps

Prerequisites

1. Admin access to the Mimecast admin console.
2. The admin must be assigned a role with read and edit API app permissions.
3. Security permissions must permit the management of app roles.

See the Mimecast documentation on Managing API 2.0 and integrations for more information.

Step 1: Create custom API App

To create a custom API app, see the Mimecast guide to Creating an API 2.0 application.

Once you finish creating the app, the Mimecast console displays the Client ID and Client Secret. Securely store these details for the next step.

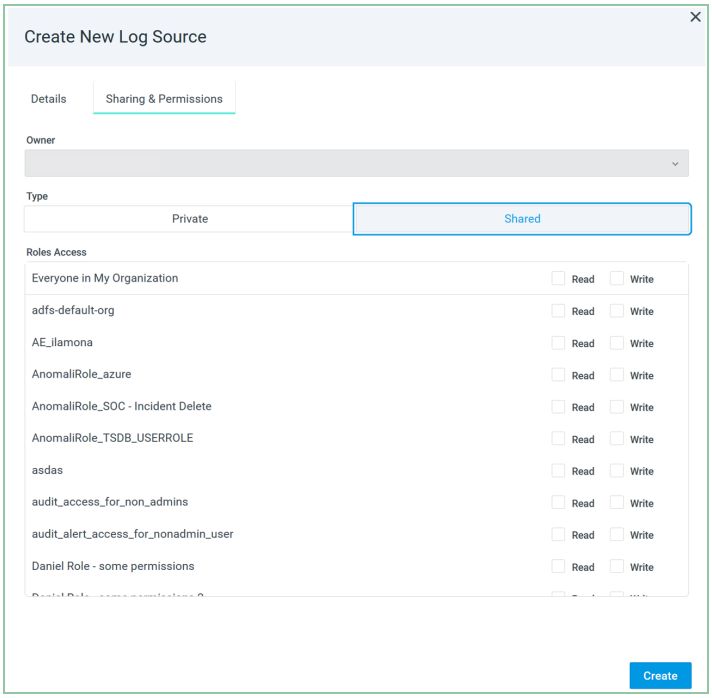
Step 2: Add Mimecast as new log source

To add Mimecast as a new log source on the Anomali platform:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select **Mimecast v2** as the source type.

6. Select **API** as the ingestion method.
7. Select API as the ingest method.
8. Provide the Basic Configuration details:
    a. **Client ID**: Enter the Client ID to authenticate requests.
    b. **Client Secret**: Enter the Client Secret to authenticate requests.
    c. (Optional) **TTP Attachment Logs**: Select whether to collect these TTP attachment logs. Enabled by default.
    d. (Optional) **TTP URL Logs**: Select whether to collect these TTP URL logs. Enabled by default.
    e. (Optional) **TTP Impersonation Logs**: Select whether to collect these TTP impersonation logs. Enabled by default.
    f. (Optional) **Rejection Logs**: Select whether to collect these rejection logs. Enabled by default.
    g. (Optional) **Threat Intel Feed**: Select whether to collect these threat intel feed logs. Disabled by default.
    h. (Optional) **Ingestion Interval**: Specify a number of minutes, hours, or days between API requests.
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:
    a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.
    b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.
10. Click **Save** to add the log source.

Step 3: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 4: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 5: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

API 1.0 call

See "Mimecast 1.0" on page 795 documentation for more information on using ingesting logs using Mimecast API 1.0.

AWS S3

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

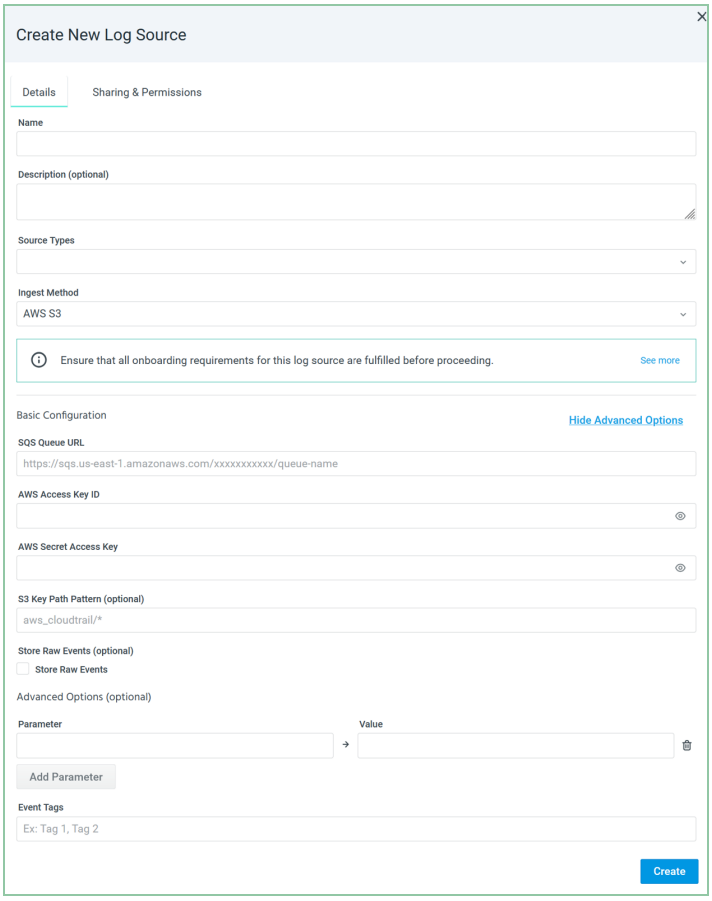
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Mimecast as new log source



On the Anomali platform, add Mimecast as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `mimecast/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"mimecast"` or `"mimecast_sourcetype"` are correct, however `"mimecast sourcetype"` is incorrect.

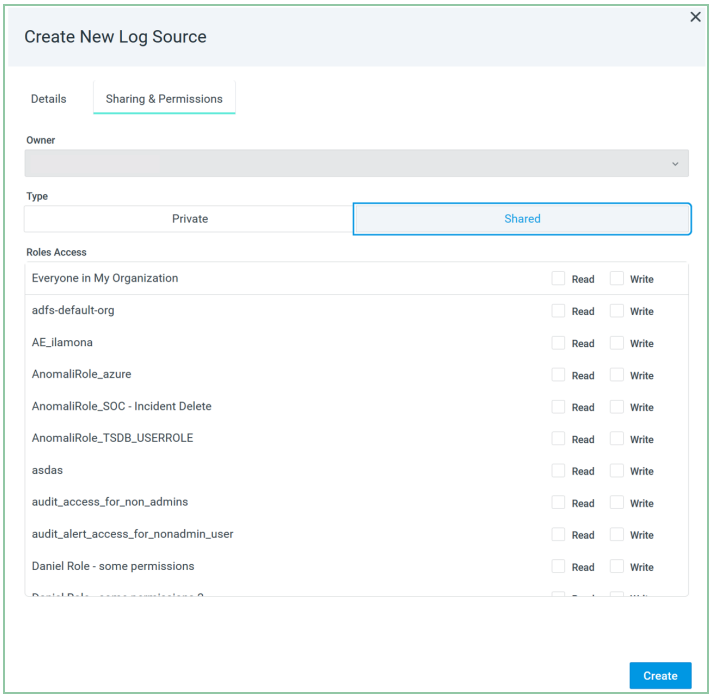
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Mimecast 1.0

> **Note:** Mimecast API 1.0 is scheduled for End of Life by end of 2026. See the official Mimecast notice for more information.

Anomali supports the ingestion of Mimecast logs through the Mimecast API 1.0 and AWS S3.

API 1.0 call

You can use your existing Mimecast Access and Secret Keys or create them to add a new log source in the Anomali platform.

Onboarding steps

Prerequisites

1. Admin access to the Mimecast admin console.
2. The admin must be assigned a role with read and edit API app permissions.
3. Security permissions must permit the management of app roles.

Step 1: Retrieve custom App ID and App Key

To create a custom API app, see the Mimecast guide to Creating an API 2.0 application and follow the Version 1.0 Integration flow instead.

After creating the app, see the Mimecast console to retrieve the App ID and App Key. Securely store these details for the next steps.

Step 2: Create new user

You must create a user profile with the correct permissions to generate API keys for Mimecast collector authentication. To create a user:

1. Sign into the admin console.
2. Navigate to the **Administration** > **Directories** > **Internal Directories** to view a list of internal domains.
3. Click the internal domain where you would like to create your new user.
4. Click **New Address** and complete the form to create a new user.
5. Keep a note of the email address and password. You will use them in "Step 7: Create Access and Secret Keys" on the next page.

Step 3: Add user to admin role

1. Navigate to **Administration** > **Account** > **Roles**.
2. Right-click the **Basic Administrator** role and click **Add users to role**.
3. Select the new user you created.
4. Click **Add selected users**.

Step 4: Create new user group

1. Navigate to **Administration** > **Directories** > **Profile Groups** menu.
2. Click the + icon on the parent folder where you would like to create the group. This creates a new group with the name **New Folder**.
3. If you prefer renaming, click the group and use the text box to change the name.
4. Navigate to **Build** > **Add Email Addresses** and enter the email address of the new user you created.
5. Click **Save and Exit**.

Step 5: Create new authentication profile

1. Navigate to **Administration** > **Services** > **Applications** menu.
2. Click **Authentication Profiles** > **New Authentication Profile**.
3. Enter a description for the new profile.

4. Set the **Authentication TTL** setting to **Never Expires**. This ensures that your token does not expire, avoiding restrictive data collection.
5. Leave other settings as default.
6. Click **Save and Exit**.

Step 6: Create new app setting

1. Navigate to **Administration** > **Services** > **Applications** menu.
2. Click **New Application Settings** > **New Authentication Profile** to enter a description.
3. In the **Group** field, paste the group you created.
4. In the **Authentication Profile** field, select the authentication profile you created.
5. Click **Save and Exit**.

Step 7: Create Access and Secret Keys

1. Navigate to **Administration** > **Services** > **API and Platform Integrations** menu.
2. Navigate to the **Your Application Integrations** tab.
3. Click the application you created, then **Create Keys**.
4. Enter the email address of the service account created in Step 2, then click **Next**.
5. In the Authentication dialog popup, enter:
   a. Type: Cloud
   b. Password: Enter the user profile password you created.
6. Click **Next**.
7. If prompted, complete the multi-factor authentication.
8. Click **Next**.
9. Securely save the Access Key and Secret Key for "Step 8: Add Mimecast as new log source" on the next page.

Step 8: Add Mimecast as new log source

To add Mimecast as a new log source on the Anomali platform:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select **Mimecast** as the source type.
6. Select **API** as the ingestion method.
7. Select API as the ingest method.
8. Provide the Basic Configuration details:
    a. **App ID**: Enter the application ID to authenticate requests.
    b. **App Key**: Enter the app key to authenticate requests.
    c. **Access Key**: Enter the access key to authenticate requests.
    d. **Secret Key**: Enter the secret key to authenticate requests.
    e. **Admin Email Address**: Email address for the service account provisioned for this integration.
        i. **Important**: The email address you specify here must be the email address associated with the service account access key provisioned for this integration.
    f. (Optional) **TTP Attachment Logs**: Select whether to collect these TTP attachment logs. Enabled by default.
    g. (Optional) **TTP URL Logs**: Select whether to collect these TTP URL logs. Enabled by default.
    h. (Optional) **TTP Impersonation Logs**: Select whether to collect these TTP impersonation logs. Enabled by default.

i. (Optional) **Threat Intel Feed**: Select whether to collect these threat intel feed logs. Enabled by default.

j. (Optional) **Ingestion Interval**: Specify a number of minutes, hours, or days between API requests.

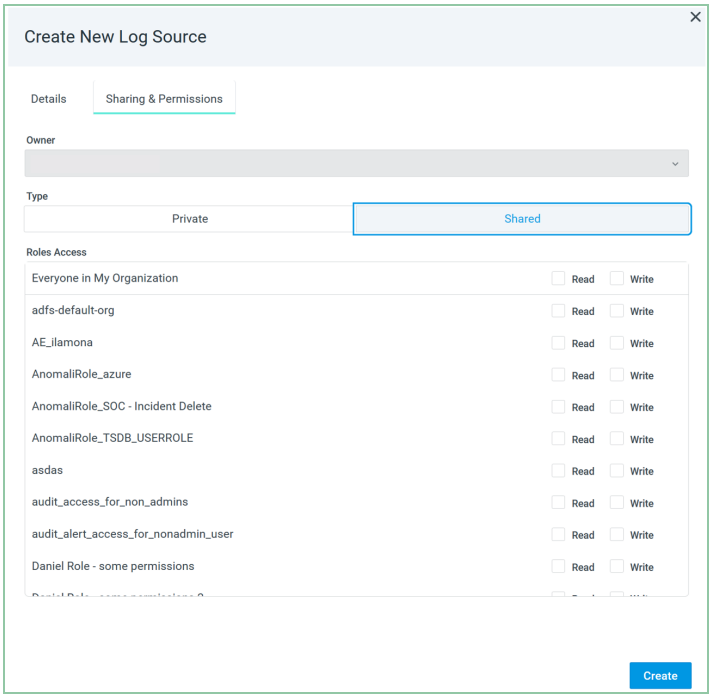
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 9: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 10: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 11: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

AWS S3

If your logs are already in S3, you can proceed directly to "Step 2: Create new user" on page 795. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

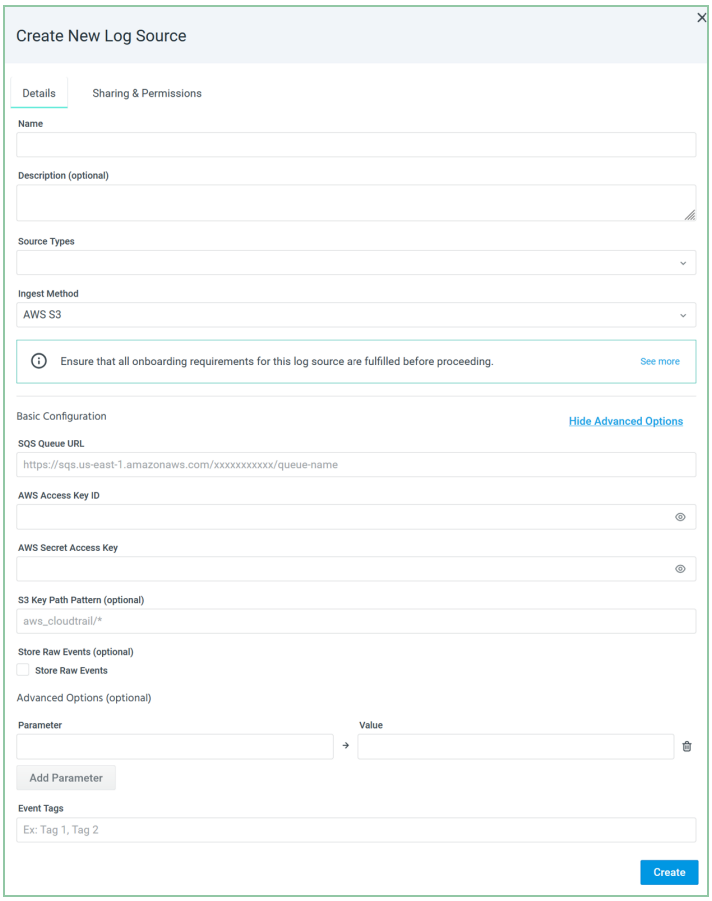
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Mimecast as new log source

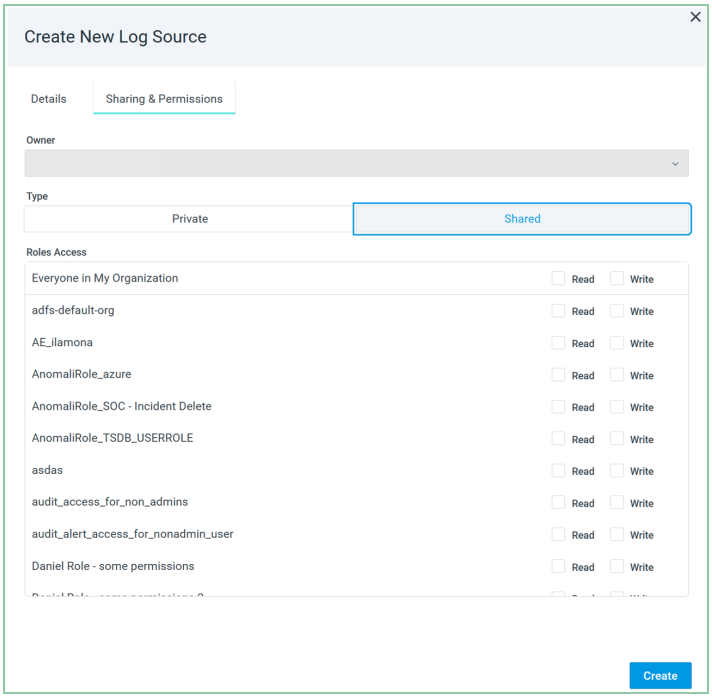


On the Anomali platform, add Mimecast as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.

5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:
   a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.
   b. **AWS Secret Access Key**: Provide the AWS secret access key.
   c. **AWS Access Key ID**: Enter the AWS Access ID.
   d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:
      - Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `mimecast/year=2025/month=03/day=22/events/event_data_logs/`.
      - Sourcetype name must not contain any spaces: For example, `"mimecast"` or `"mimecast_sourcetype"` are correct, however `"mimecast sourcetype"` is incorrect.
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:
   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.
   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.
10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Microsoft DHCP

Anomali supports the ingestion of Microsoft DHCP logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

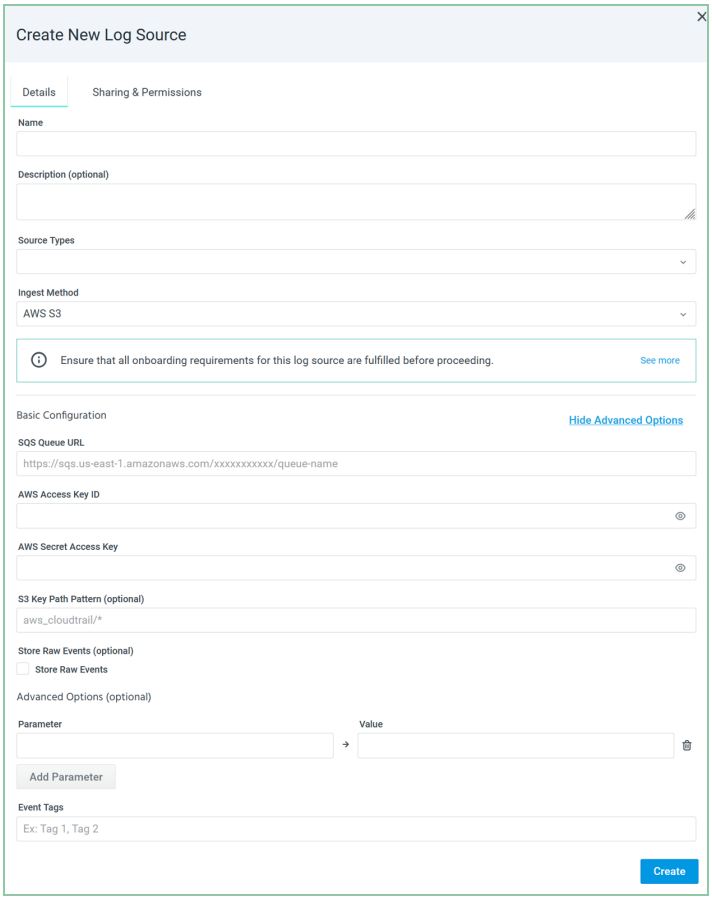
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Microsoft DHCP as new log source



On the Anomali platform, add Microsoft DHCP as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `ms_dhcp/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"ms_dhcp"` is correct, however `"Microsoft DHCP"` is incorrect.

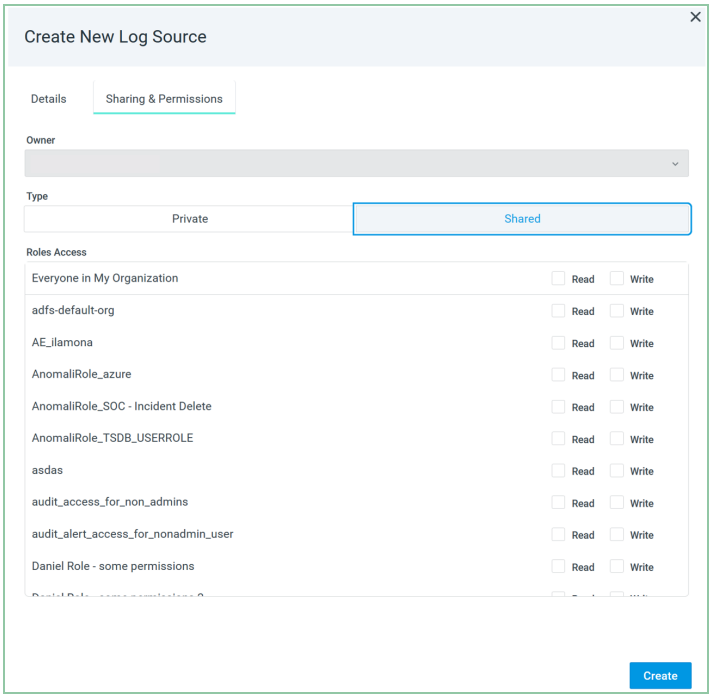
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Microsoft Graph Security Alert

Anomali supports the ingestion of MS Graph Security Alert logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

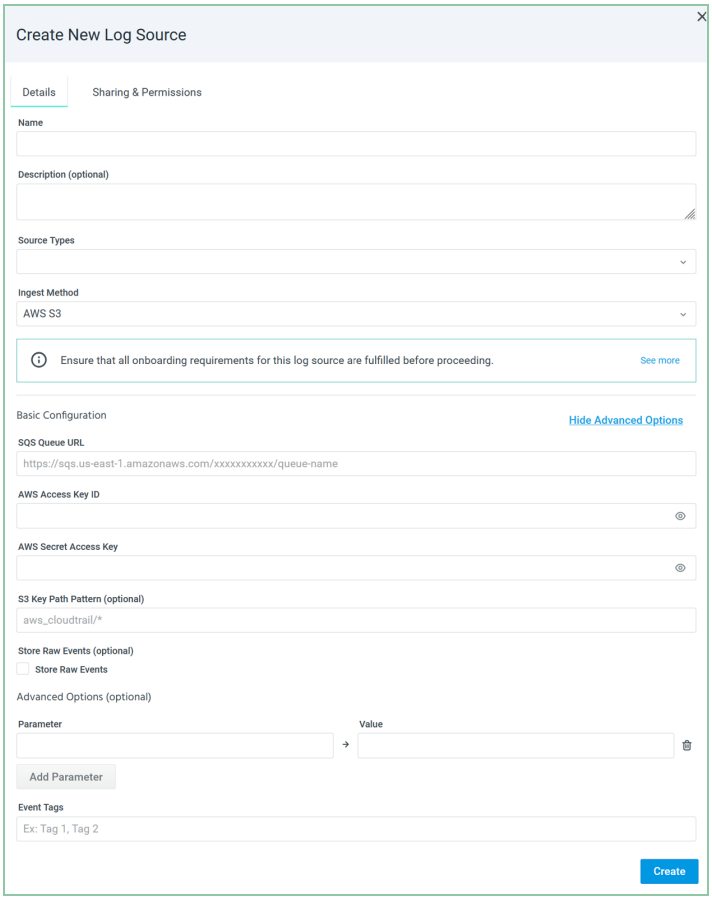
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Graph Security Alert as new log source



On the Anomali platform, add MS Graph Security Alert as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `ms_graph_sec_alert/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"ms_graph_sec_alert"` is correct, however `"ms graph sec alert"` is incorrect.

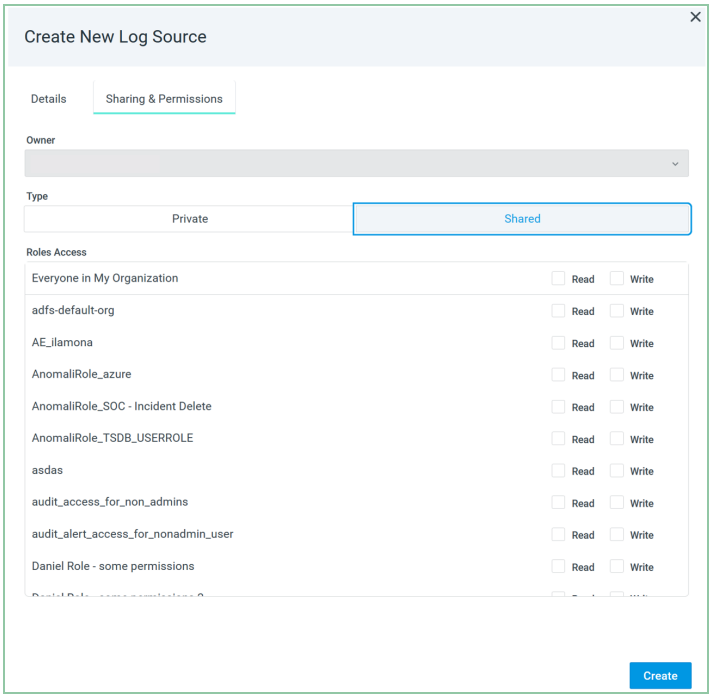
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Miro Audit

Anomali supports the ingestion of Miro Audit logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

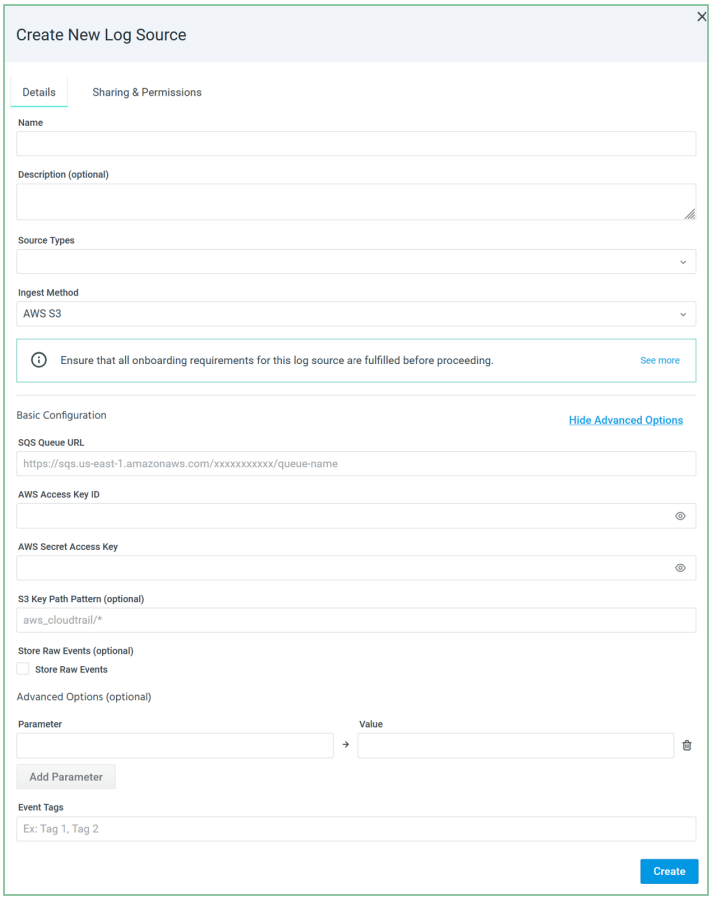
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Miro Audit as new log source



On the Anomali platform, add Miro Audit as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `miro_audit/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"miro_audit"` is correct, however `"Miro Audit"` is incorrect.

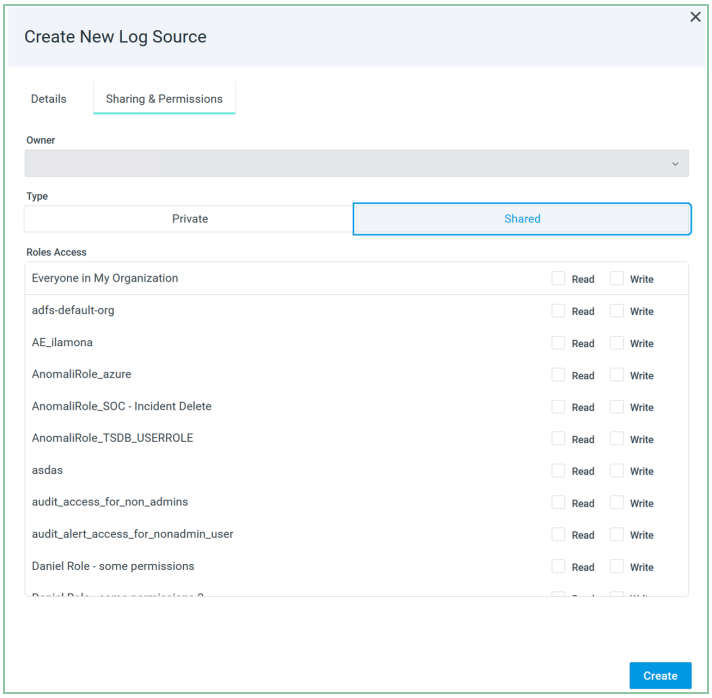
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Microsoft Cluster Services Audit

Anomali supports the ingestion of Microsoft Cluster Services (MSCS) Audit logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

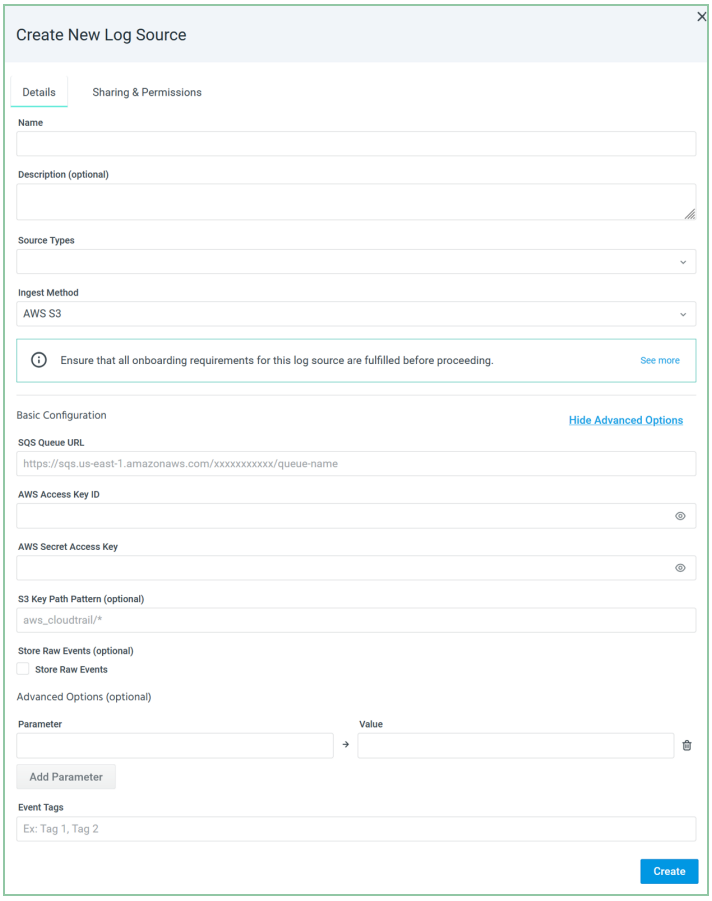
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add MSCS Audit as new log source



On the Anomali platform, add MSCS Audit as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `mscs_audit/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"mscs_audit"` is correct, however `"mscs audit"` is incorrect.

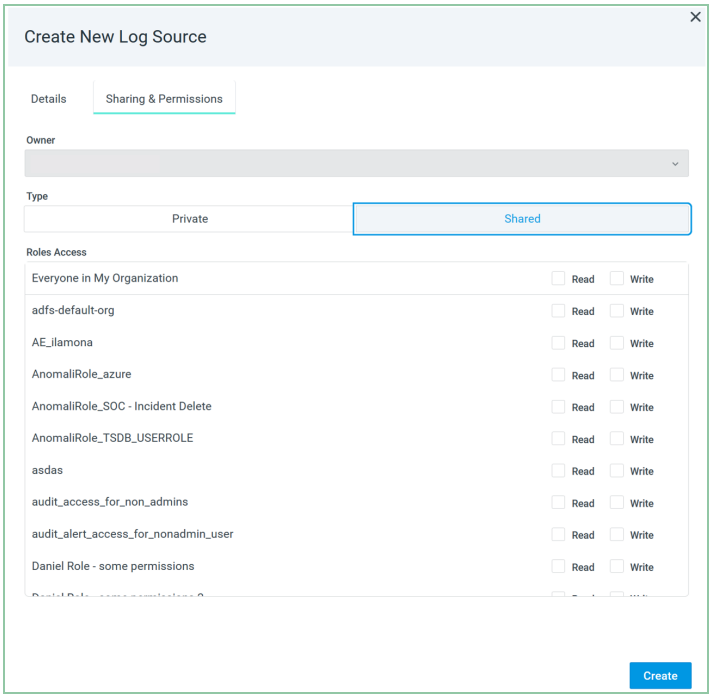
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Microsoft Cluster Services Azure

Anomali supports the ingestion of Microsoft Cluster Services Azure logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

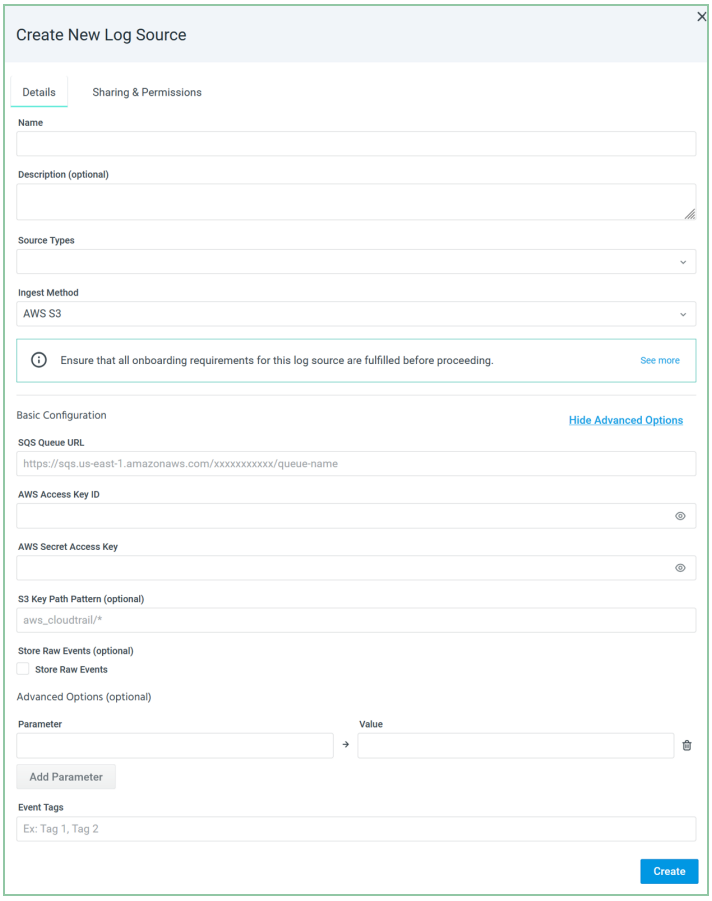
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add MSCS Azure as new log source



On the Anomali platform, add MSCS Azure as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `mscs_azure/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"mscs_azure"` is correct, however `"MSCS Azure"` is incorrect.

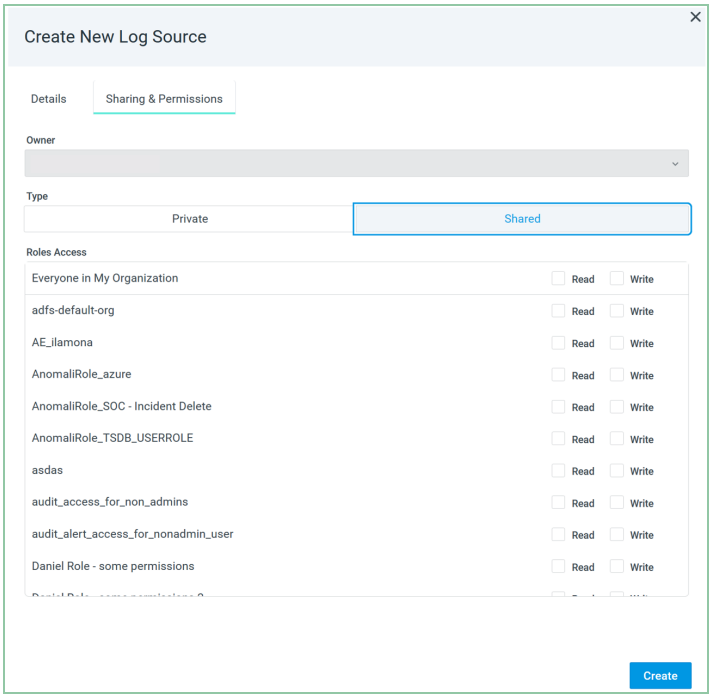
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Nametag

Anomali supports the ingestion of Nametag logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

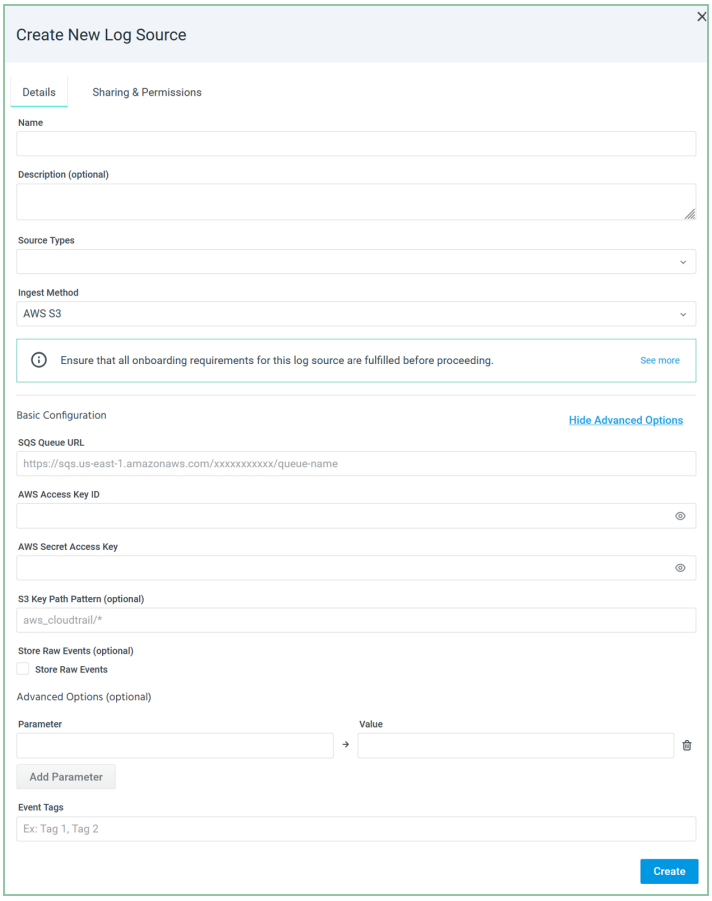
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Nametag as new log source



On the Anomali platform, add Nametag as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `nametag/year=2025/month=03/day=22/events/event_data_logs/`.

- Sourcetype name must not contain any spaces: For example, `"nametag"` or `"nametag_sourcetype"` are correct, however `"Nametag Sourcetype"` is incorrect.

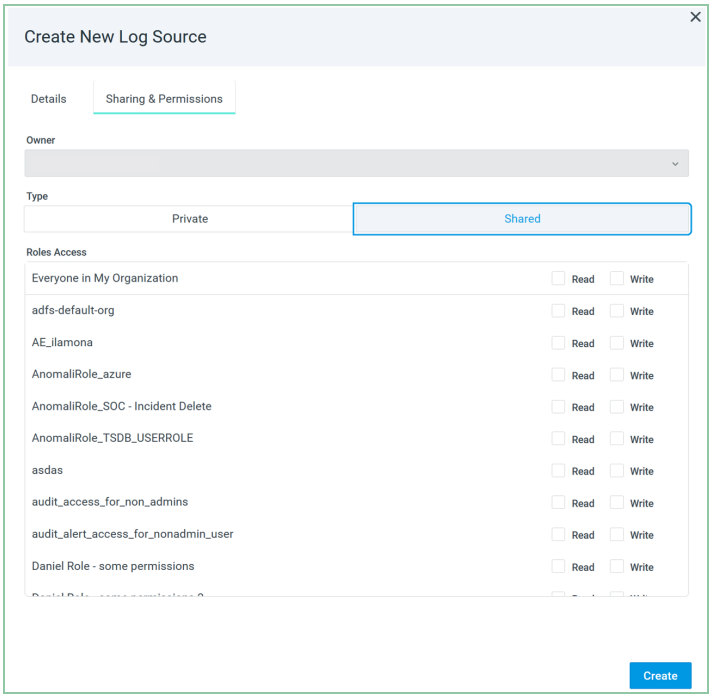
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Nasuni Log

Anomali supports the ingestion of Nasuni Log logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

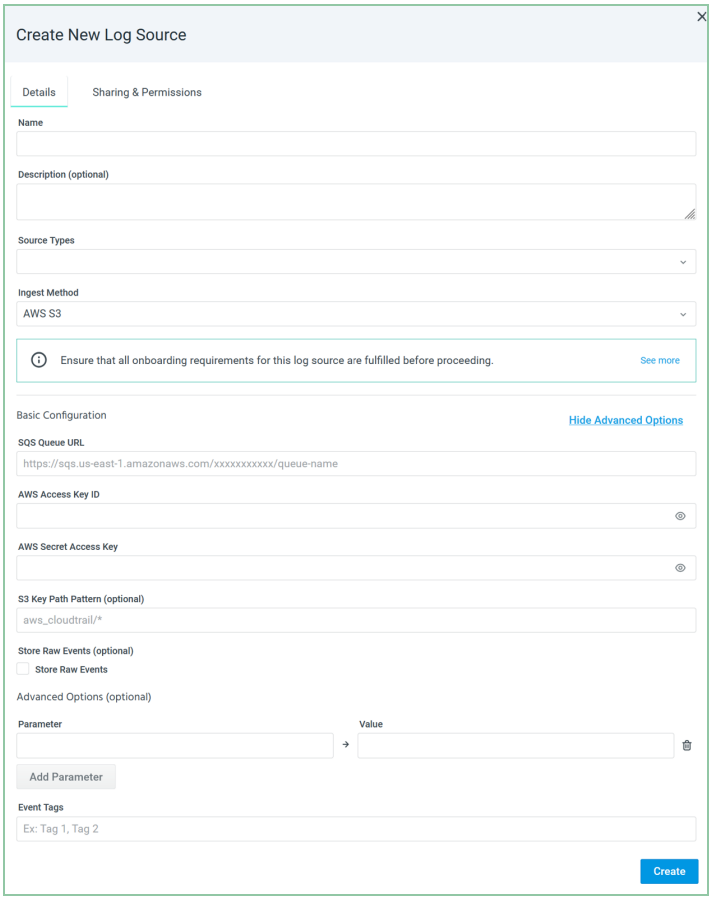
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Nasuni Log as new log source



On the Anomali platform, add Nasuni Log as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `nasuni_log/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"nasuni_log"` is correct, however `"Nasuni Log"` is incorrect.

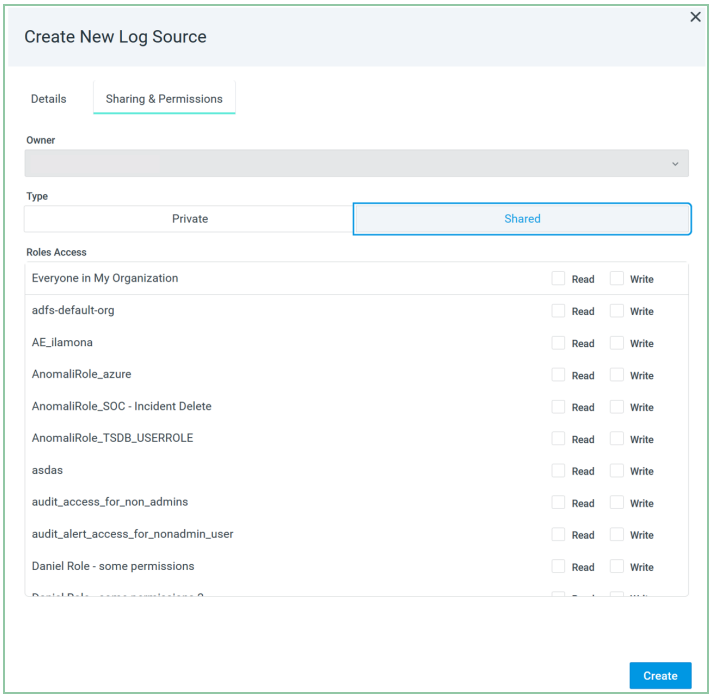
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Nasuni Storage

Anomali supports the ingestion of Nasuni Storage logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

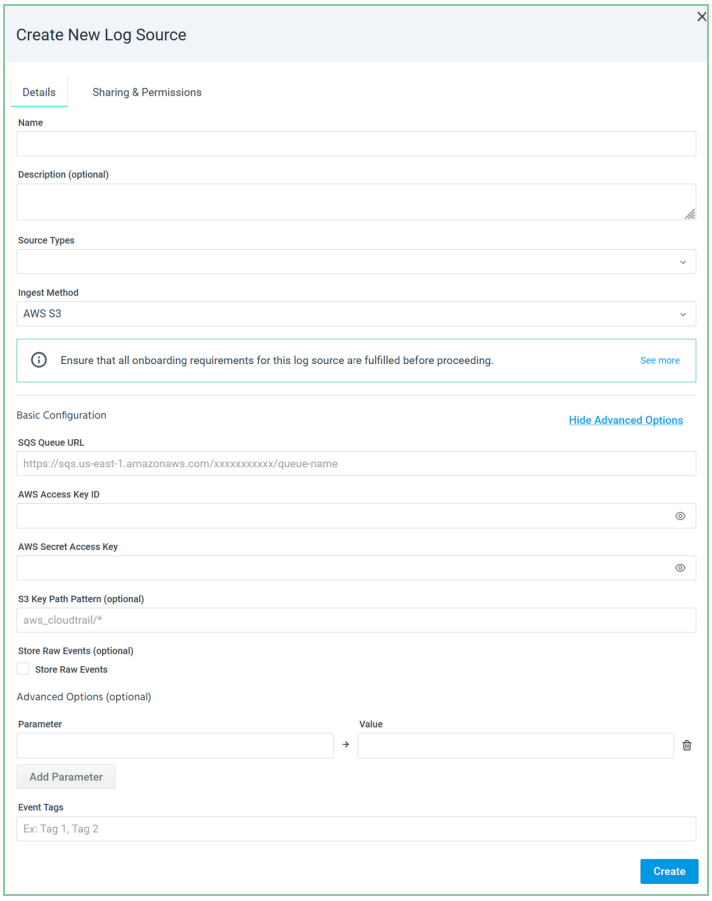
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Nasuni Storage as new log source



On the Anomali platform, add Nasuni Storage as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `nasuni_storage/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"nasuni_storage"` is correct, however `"Nasuni Storage"` is incorrect.

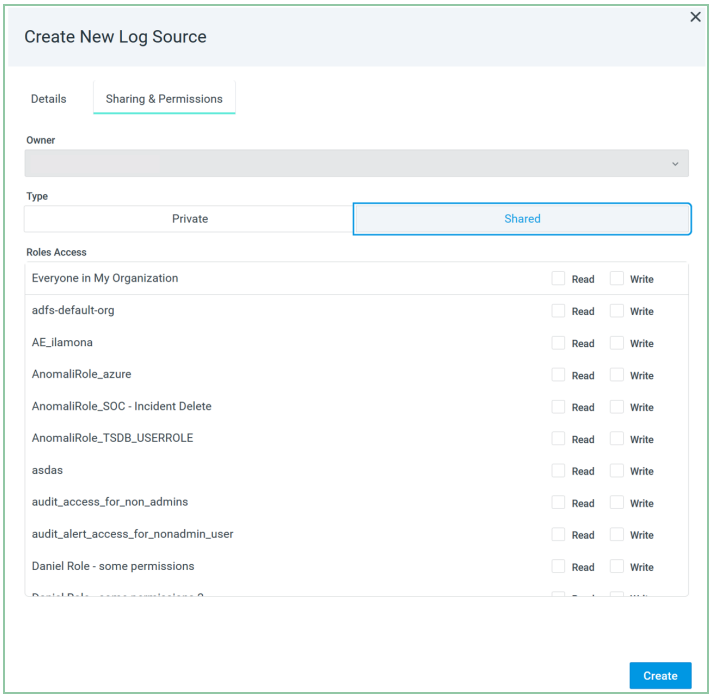
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Netskope

Anomali supports the ingestion of Netskope logs through the Netskope "REST API v2" below and AWS S3.

REST API v2

You can use your existing API token or create a new token to add a new log source in the Anomali platform.

Onboarding steps

Step 1: Create API token

1. Sign into the Netskope admin console.
2. Navigate to **Settings** > **Tools** > **REST API v2**.
3. Click **New token**.
4. Enter a name and provide the scope as well as expiry date for the token. Securely store the token value for the subsequent steps.
5. Click **Save**.

Step 2: Add Netskope as a new log source

To add Netskope as a new log source on the Anomali platform:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select **Netskope** as the source type.
6. Select **API** as the ingestion method.
7. Select API as the ingest method.
8. Provide the Basic Configuration details:

a. **URL**: Enter your existing token ID or the new token you created in "Step 1: Create API token" on the previous page.

b. **Access Key**: Enter your Okta domain name.

c. (Optional) **Ingestion interval**: Select the ingestion interval schedule (in minutes, hours, and days).

d. (Optional) **Offset**: Enter the offset value. Default is 10.

e. (Optional) **Limit**: Enter the limit value. Default is 10.

f. (Optional) **Alerts**: Select whether to enable any alerts for your ingestion. Enabled by default.

g. (Optional) **Applications**: Select whether to enable any applications. Enabled by default.

h. (Optional) **Audit**: Select whether to enable any audits for your ingestion. Enabled by default.

i. (Optional) **Infrastructure**: Select whether to enable infrastructure. Enabled by default.

j. (Optional) **Network**: Select whether to enable network. Enabled by default.

k. (Optional) **Page**: Select whether to enable page. Enabled by default.

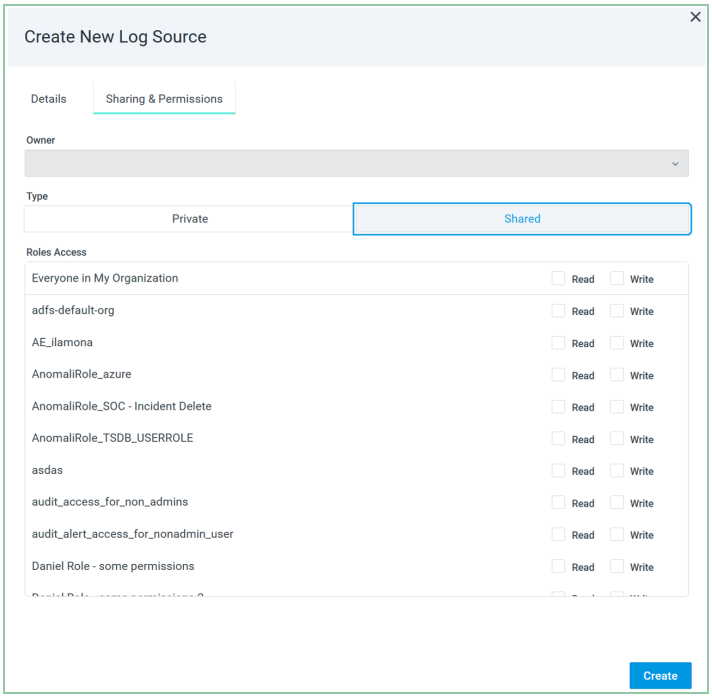
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 3: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 4: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 5: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

AWS S3

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

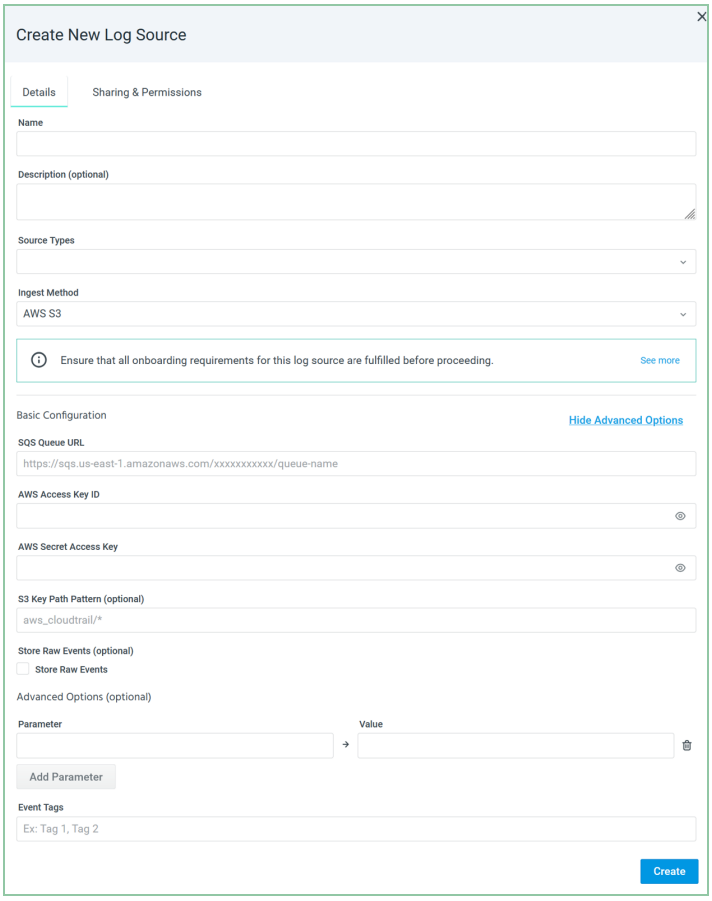
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Netskope as new log source



On the Anomali platform, add Netskope as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `netskope/year=2025/month=03/day=22/events/event_data_logs/`.

- Sourcetype name must not contain any spaces: For example, `"netskope"` or `"netskope_sourcetype"` are correct, however `"netskope sourcetype"` is incorrect.

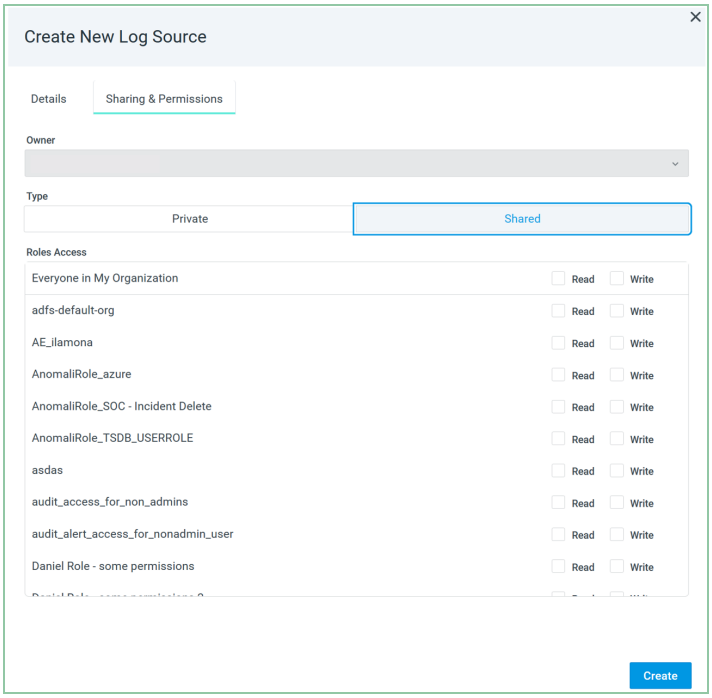
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

NSG Flow

Anomali supports the ingestion of NSG Flow logs through the Azure Storage Account.

Azure Storage Account

You can use your existing Azure Storage Account or create a new Azure Storage Account to add a new log source in the Anomali platform.

Onboarding steps

Prerequisites

1. An active Azure subscription.

Step 1: Register Insights Provider

See Microsoft's guide to Register Insights Provider for more information.

Step 2: Azure storage account

If you don't have an Azure storage account, see Microsoft's guide to Create an Azure storage account.

If the account exists, proceed to "Step 3: Obtain Account Access Key" below.

Step 3: Obtain Account Access Key

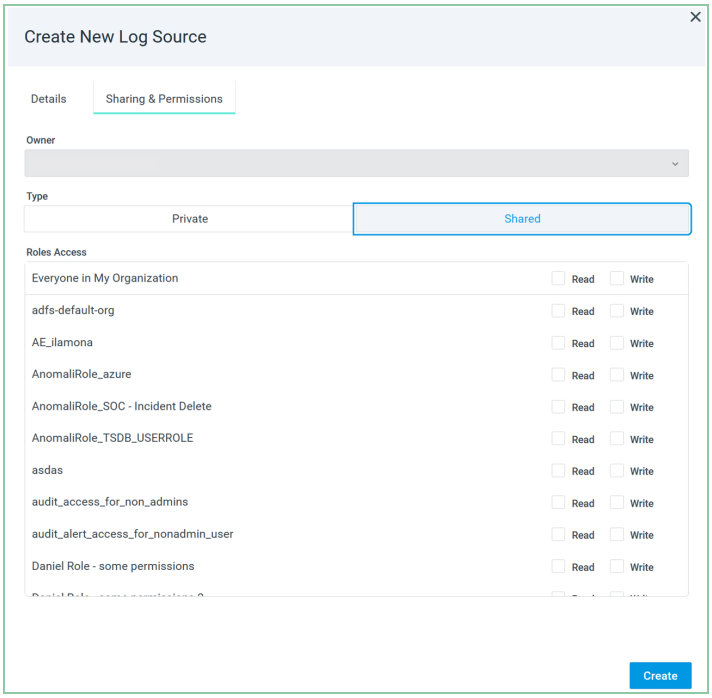
1. Sign into the Azure portal.
2. Navigate to **Storage account** and select your account.
3. In the **Security + networking** section, navigate to the **Access keys** setting.
4. Click **Show Keys**.
5. Copy the access key and note the corresponding **Storage Account Name**.

Step 4: Add NSG Flow as new log source

To add NSG Flow as a new log source on the Anomali platform:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select **NSG Flow** as the source type.
6. Select **API** as the ingestion method.
7. Select API as the ingest method.
8. Provide the Basic Configuration details:
   a. **Azure Storage Account Name**: Enter the storage account name you obtained in "Step 3: Obtain Account Access Key" on the previous page.
   b. **Azure Storage Account Access Key**: Enter the account access key you obtained in "Step 3: Obtain Account Access Key" on the previous page.
   c. **Wildcard Log Schema**: Provide the wildcard log schema.
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:
   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.
   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.
10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

NXLog Agent

Anomali supports the ingestion of NXLog Agent logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

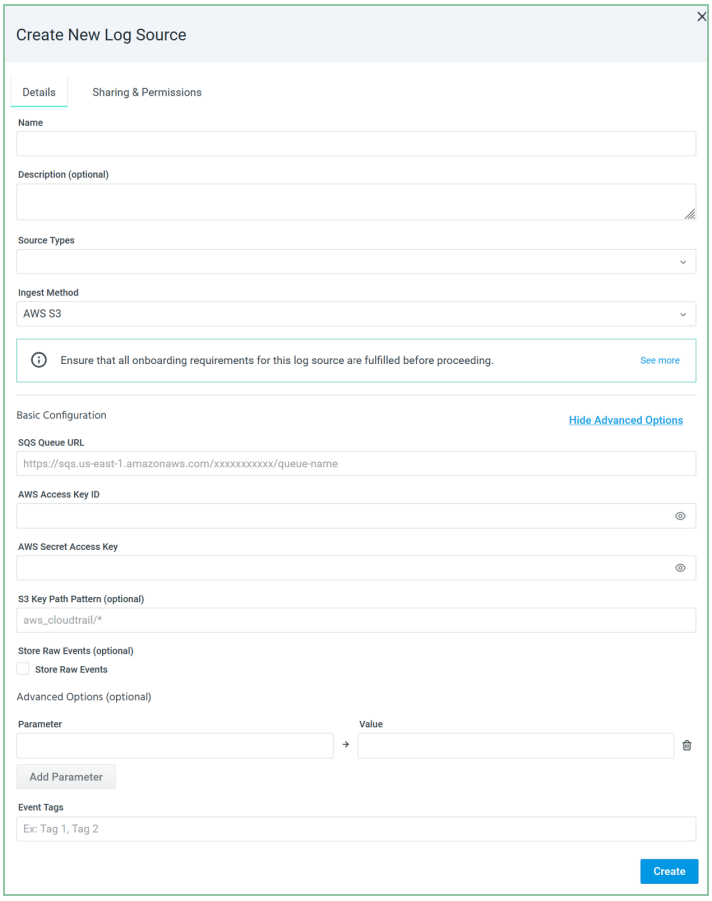
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add NXLog Agent as new log source



On the Anomali platform, add NXLog Agent as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `NXLog_agent/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"NXLog_agent"` is correct, however `"NXLog Agent"` is incorrect.

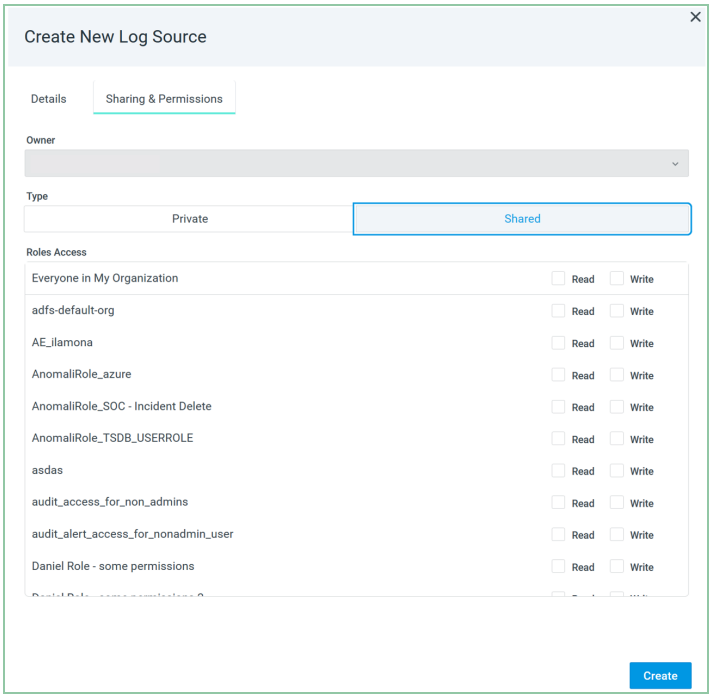
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Microsoft Office 365

Anomali Security Analytics can ingest event logs from Office 365 through the "Management Activity API" below and "AWS S3" on page 865.

Management Activity API

Onboarding steps

Prerequisites

You must enable audit logging for your Microsoft 365 tenancy through the Security and Compliance Center in the Office 365 Admin Portal. See Microsoft's guide to turning on auditing for more information.

Step 1: Register an App with Azure AD

1. Sign into the Microsoft Entra admin center.
2. Navigate to **Identity** > **Applications** > **App registrations**.
3. Click **New Registration**.
4. Enter a display name. For example, `Office 365 Integration with Anomali`.
5. Select **Accounts in this organizational directory** as the supported account type.
6. Click **Register**.
7. Click **Manage** > **Certificates and Secrets** > **New Client Secret**.
8. Add a description and set the expiry date for the certificate, then click **Add**. Securely save the Client Secret value for subsequent steps.
9. Configure API permissions:
   a. In the left menu, click **API permissions** > **Add a permission** > **Office 365 Management APIs**.
   b. Click **Application permissions** and select all the available permissions. The following permissions must be selected:

- Read activity data from your organization
- Read DLP policy events including detected sensitive data
- Read service health information from your organization

c. Click **Add permissions**.

d. In the API permissions page, click **Grant admin consent** for your organization and then click **Yes**.

10. Once consent has been granted, navigate to the **Overview** tab to view the following details you must provide to Anomali for log ingestion:

    a. **Application (Client) ID**

    b. **Directory (Tenant) ID**

Step 2: Add Office 365 as new log source

To add Office 365 as a new log source on the Anomali platform:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select **Office 365** as the log source type.
6. Select **API** as the ingestion method.
7. Select API as the ingest method.
8. Provide the Basic Configuration details, from "Microsoft Office 365 " on the previous page:

    a. **Client ID**: Application (client) ID of the Azure AD application.

    b. **Client Secret**: Application (client) Secret associated with the Application ID above.

c. **Tenant ID**: Tenant ID assigned to your organization in Active Directory.

d. **Log Schema**: Enter the log schema.

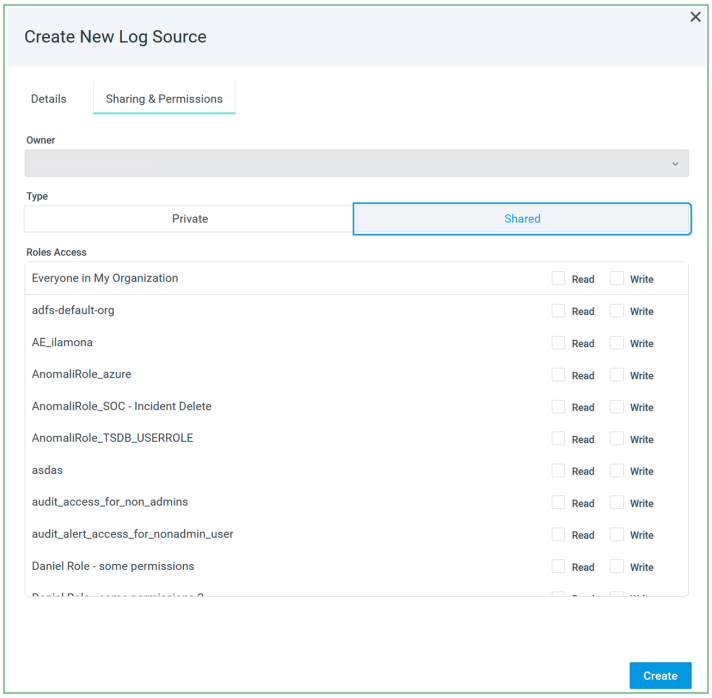
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 3: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.

2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 4: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 5: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

AWS S3

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

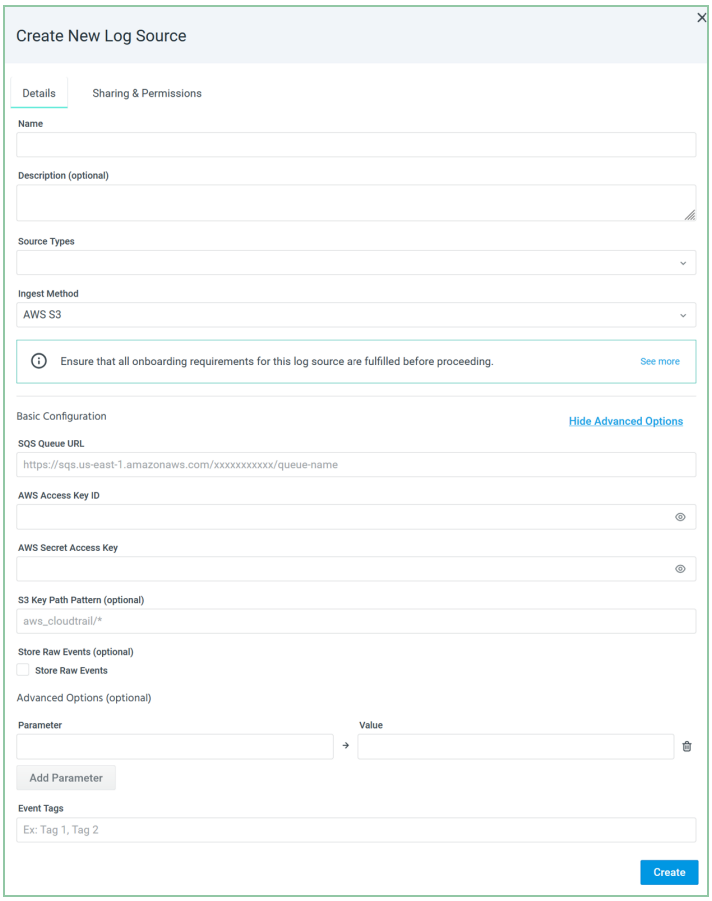
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Office365 as new log source

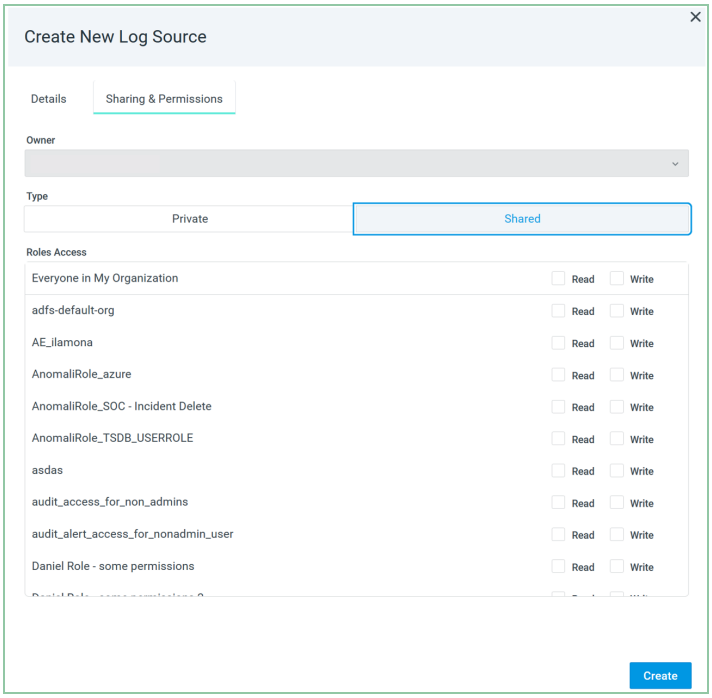


On the Anomali platform, add Office365 as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.

5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:
   a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.
   b. **AWS Secret Access Key**: Provide the AWS secret access key.
   c. **AWS Access Key ID**: Enter the AWS Access ID.
   d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:
      - Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `office365/year=2025/month=03/day=22/events/event_data_logs/`.
      - Sourcetype name must not contain any spaces: For example, `"office365"` or `"office365_sourcetype"` are correct, however `"office365 sourcetype"` is incorrect.
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:
   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.
   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.
10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Microsoft Office365 Graph

Anomali supports the ingestion of Office365 Graph logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

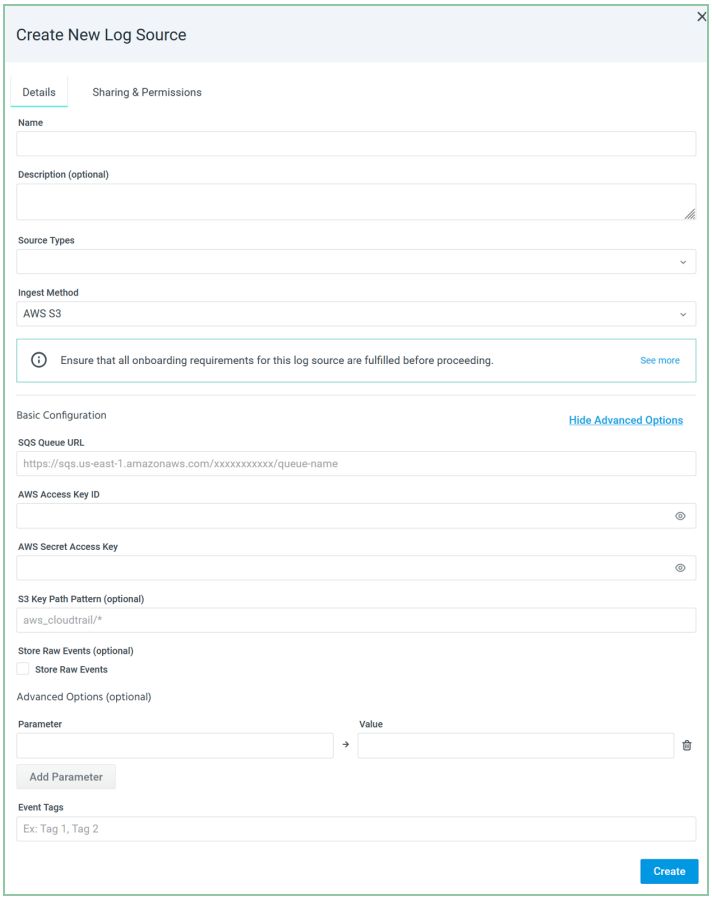
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Office365 Graph as new log source



On the Anomali platform, add Office365 Graph as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `office365_graph/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"office365_graph"` is correct, however `"Office365 Graph"` is incorrect.

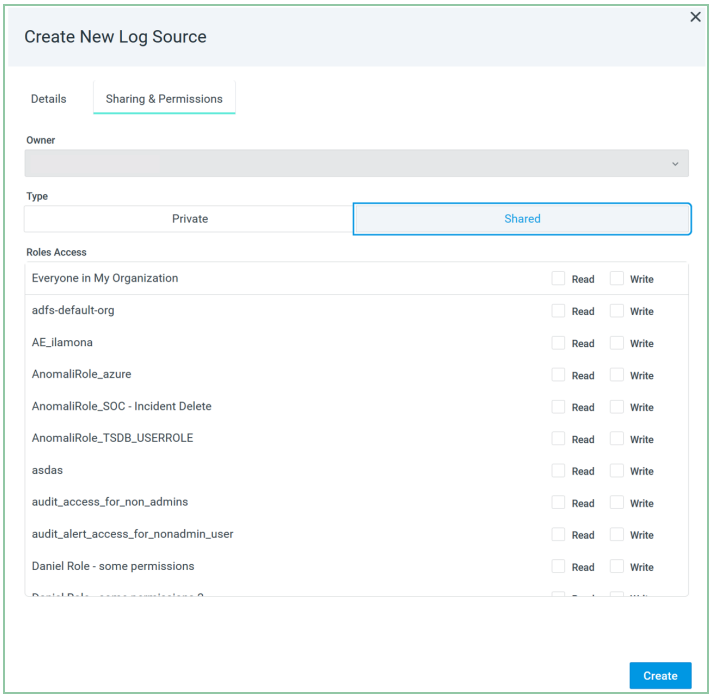
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Okta

Anomali supports the ingestion of Okta logs either through the Okta System Log API or "AWS S3" on page 877.

System Log API

You can use your existing API token or create a new token along with your domain and subdomain to add a new log source in the Anomali platform.

Onboarding steps

Step 1: Create API token

1. Sign into the Okta admin console.
2. Navigate to **Security** > **API**.
3. Click **Create Token**.
4. Enter a name for the token. For example, `Anomali API token`.
5. Securely store the token value for the subsequent steps.

Step 2: Add Okta as a new log source

To add Okta as a new log source on the Anomali platform:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select **Okta** as the log source type.
6. Select **API** as the ingestion method.
7. Select API as the ingest method.
8. Provide the Basic Configuration details:

a. **Token**: Enter your existing token ID or the new token you created in "Step 1: Create API token" on the previous page.

b. **Okta domain**: Enter your Okta domain name.

c. **Enabled event types**: Provide all the Okta event types you would like to ingest into Anomali.

d. **PRTG domain**: Enter the PRTG fully qualified domain name or IP address from which Anomali can pull your logs.

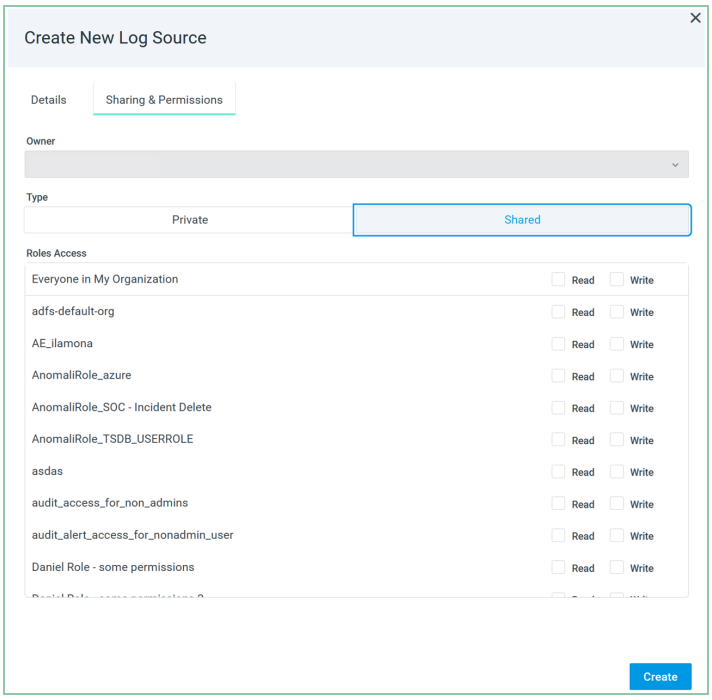
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 3: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 4: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 5: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

AWS S3

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" on the next page. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

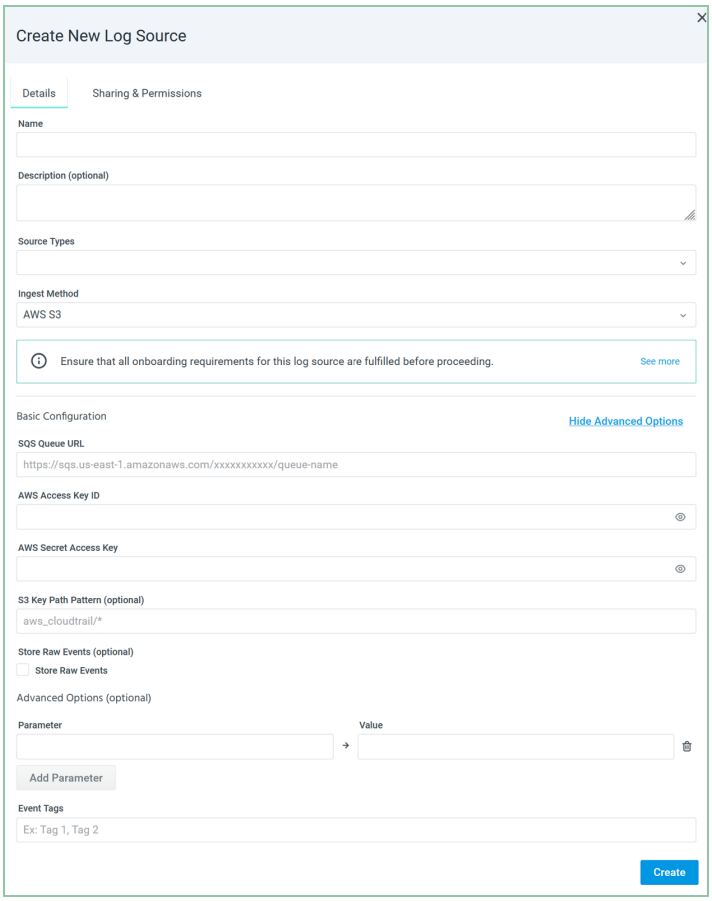
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Okta as new log source

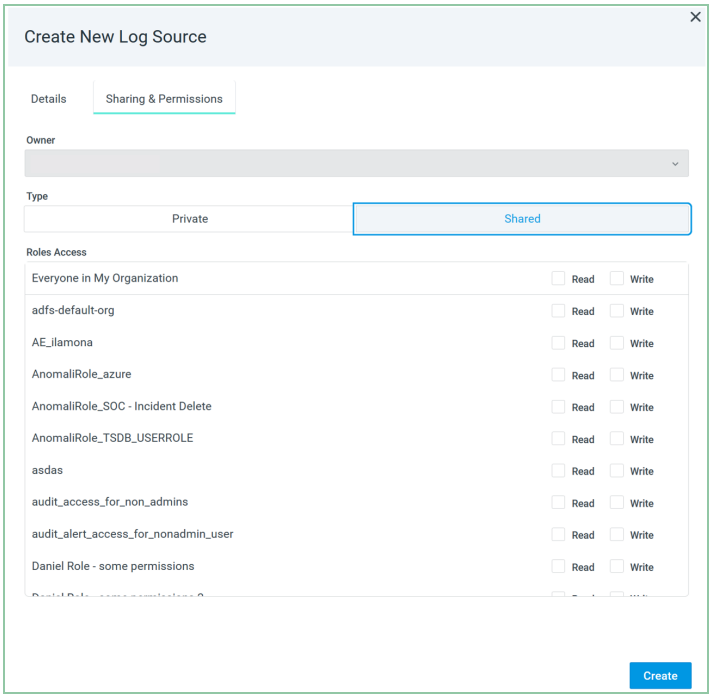


On the Anomali platform, add Okta as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.

3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:
   a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.
   b. **AWS Secret Access Key**: Provide the AWS secret access key.
   c. **AWS Access Key ID**: Enter the AWS Access ID.
   d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:
      - Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `okta/year=2025/month=03/day=22/events/event_data_logs/`.
      - Sourcetype name must not contain any spaces: For example, `"okta"` or `"okta_sourcetype"` are correct, however `"okta sourcetype"` is incorrect.
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:
   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.
   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.
10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Okta Agent

Anomali supports the ingestion of Okta Agent logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

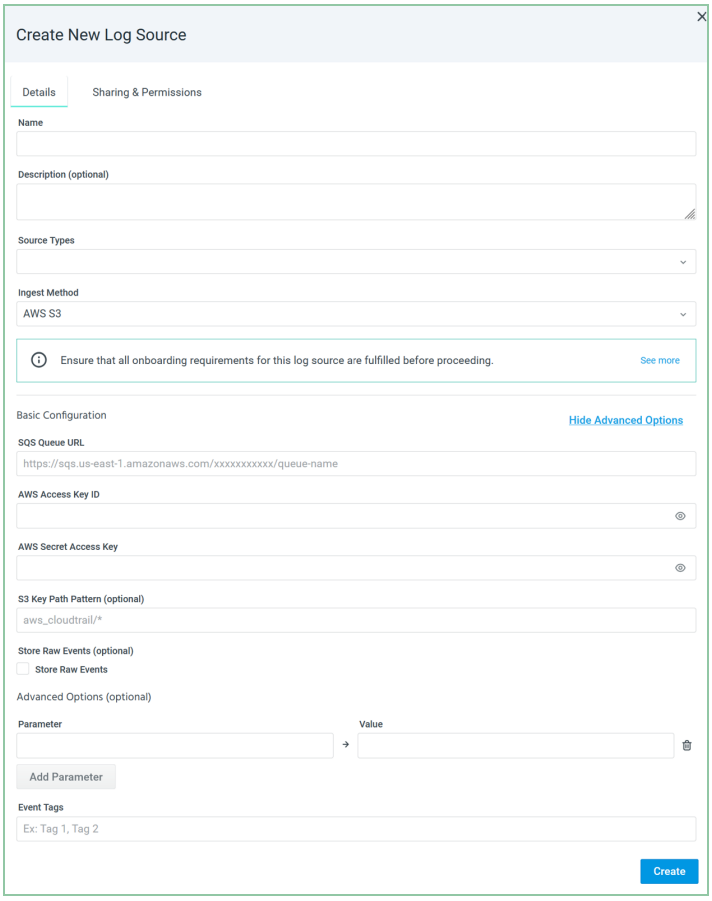
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Okta Agent as new log source



On the Anomali platform, add Okta Agent as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `okta_agent/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"okta_agent"` is correct, however `"Okta Agent"` is incorrect.

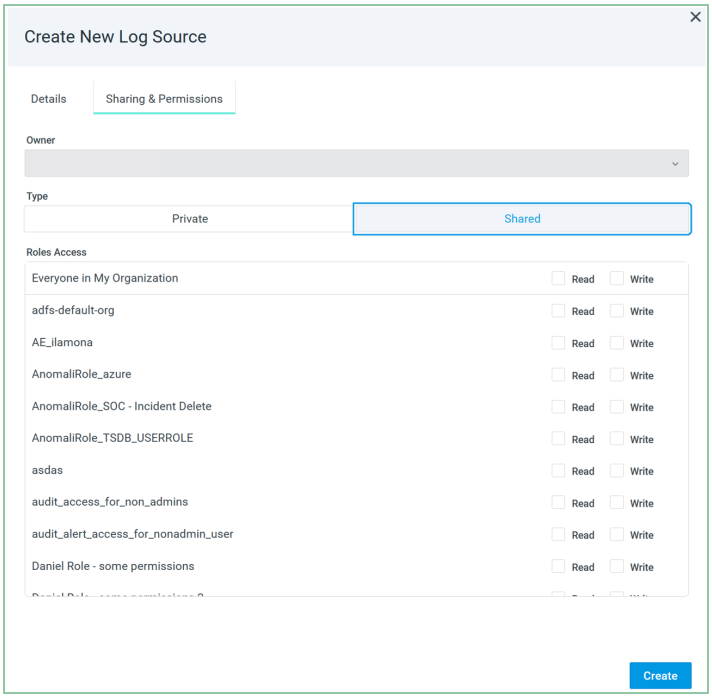
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Okta Radius

Anomali supports the ingestion of Okta Radius logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

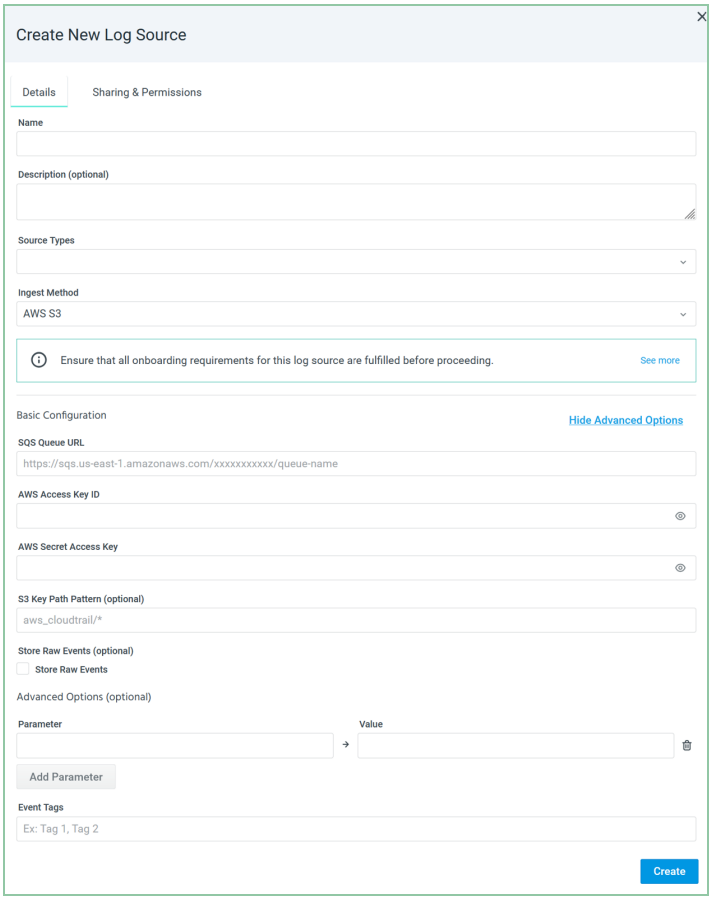
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Okta Radius as new log source



On the Anomali platform, add Okta Radius as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `okta_radius/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"okta_radius"` is correct, however `"Okta Radius"` is incorrect.

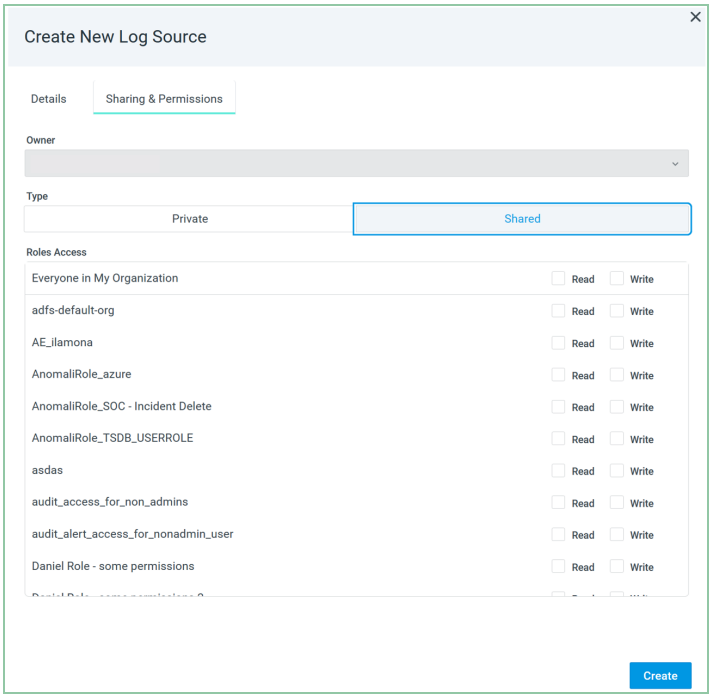
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Okta Radius Access

Anomali supports the ingestion of Okta Radius Access logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

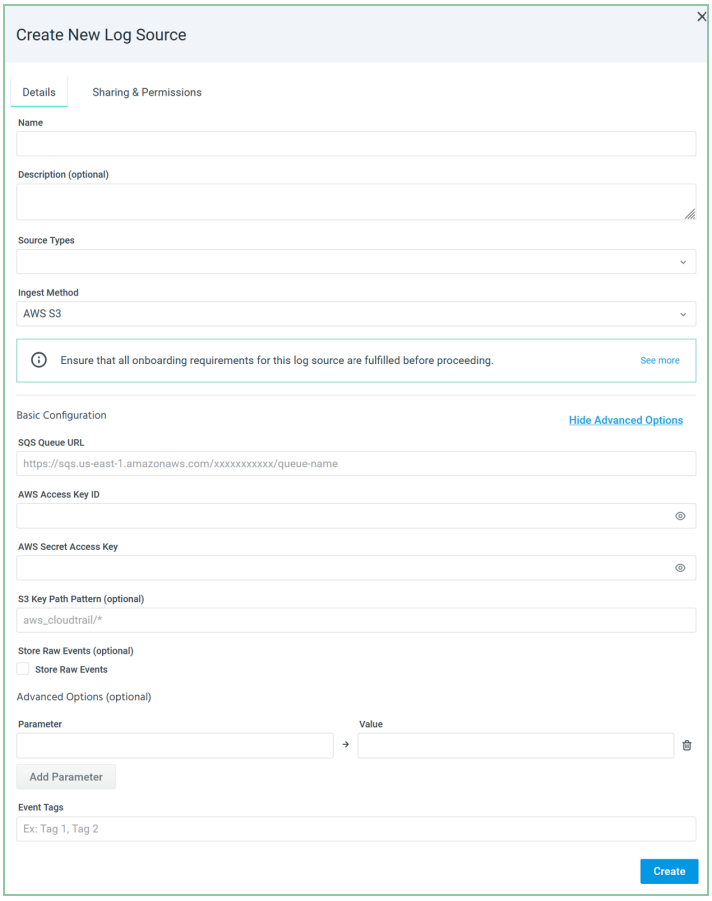
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Okta Radius Access as new log source



On the Anomali platform, add Okta Radius Access as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `okta_radius_access/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"okta_radius_access"` is correct, however `"Okta Radius Access"` is incorrect.

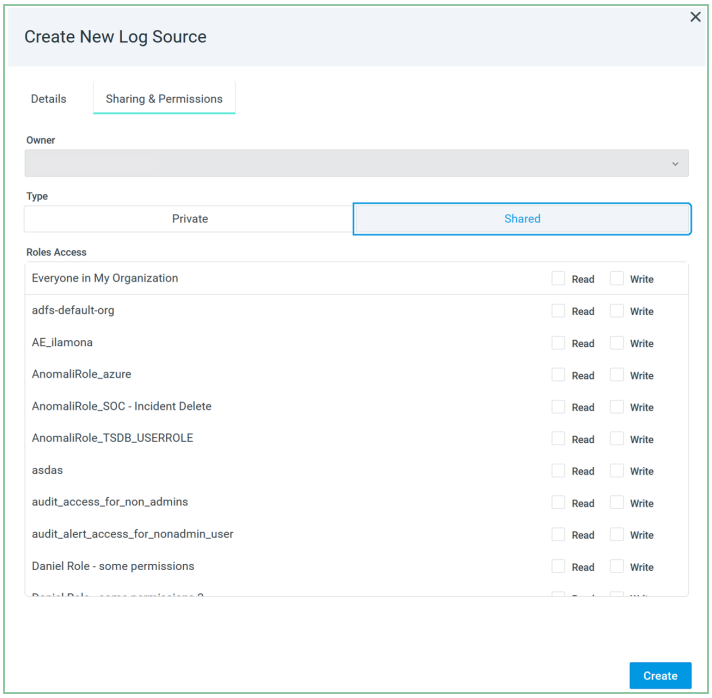
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Oracle IAM Access

Anomali supports the ingestion of Oracle IAM Access logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

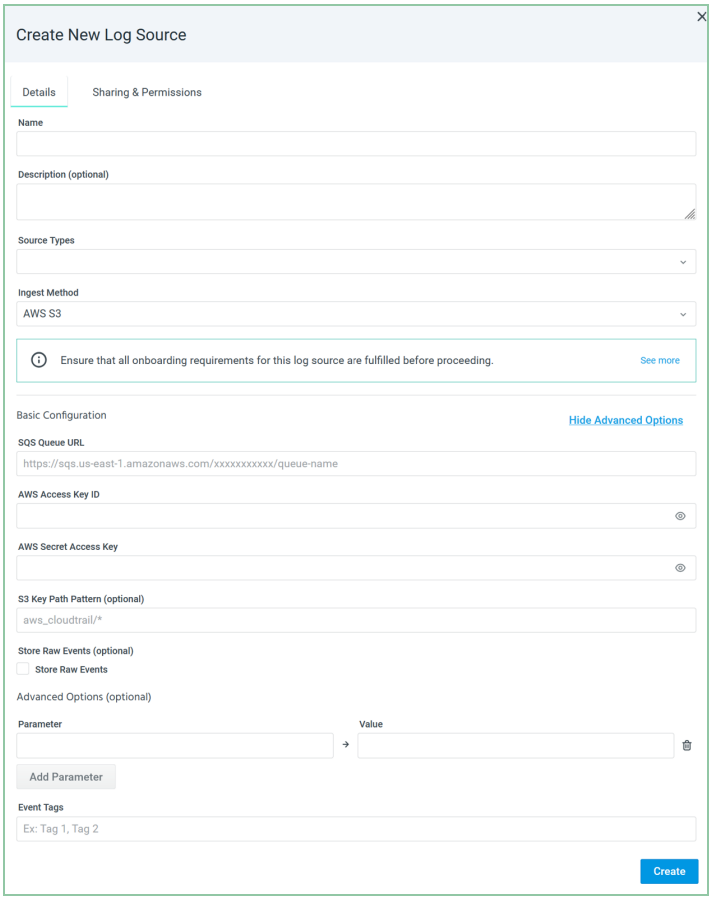
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Oracle IAM Access as new log source



On the Anomali platform, add Oracle IAM Access as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `oracle_iam_access/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"oracle_iam_access"` is correct, however `"Oracle IAM Access"` is incorrect.

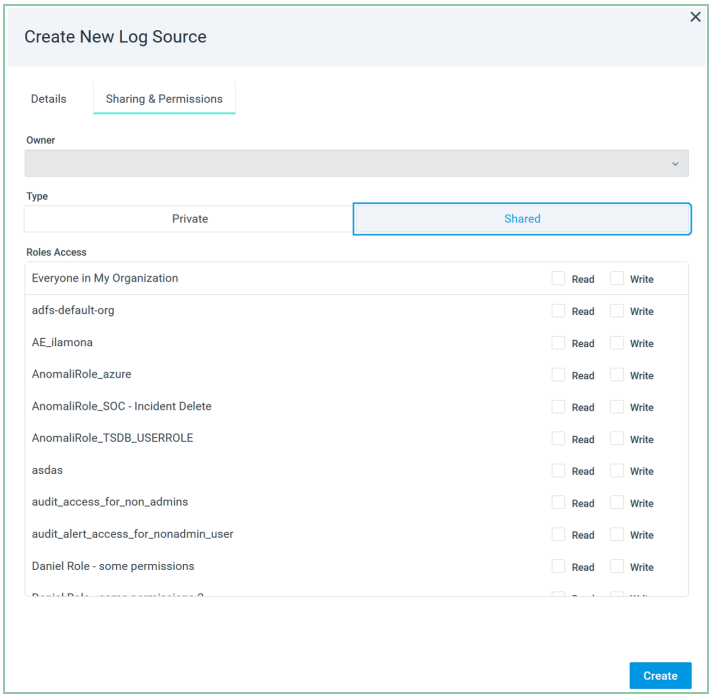
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Oracle IAM Errors

Anomali supports the ingestion of Oracle IAM Error logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

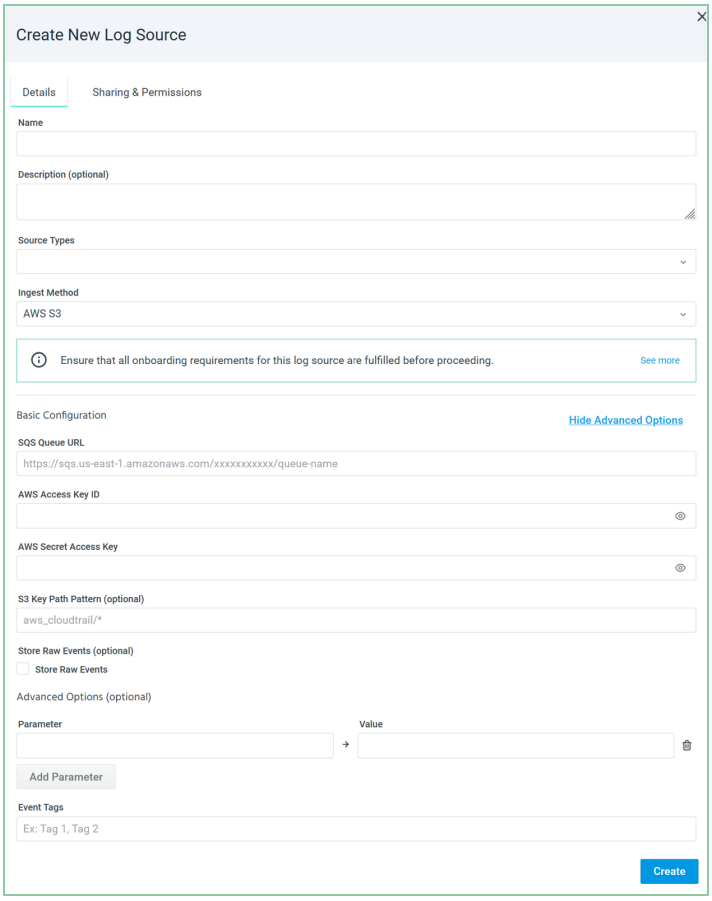
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Oracle IAM Error as new log source



On the Anomali platform, add Oracle IAM Error as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `oracle_iam_error/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"oracle_iam_error"` is correct, however `"Oracle IAM Error"` is incorrect.

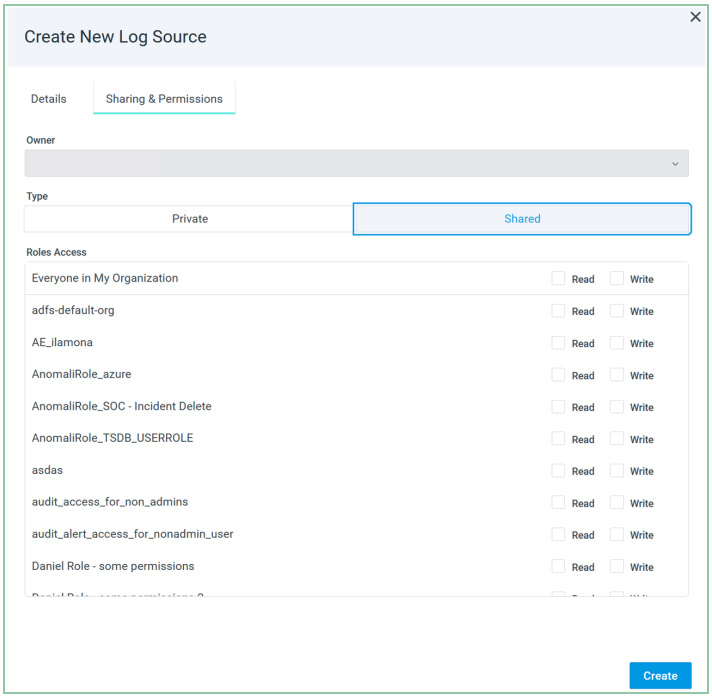
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Oracle IAM Replication

Anomali supports the ingestion of Oracle IAM Replication logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

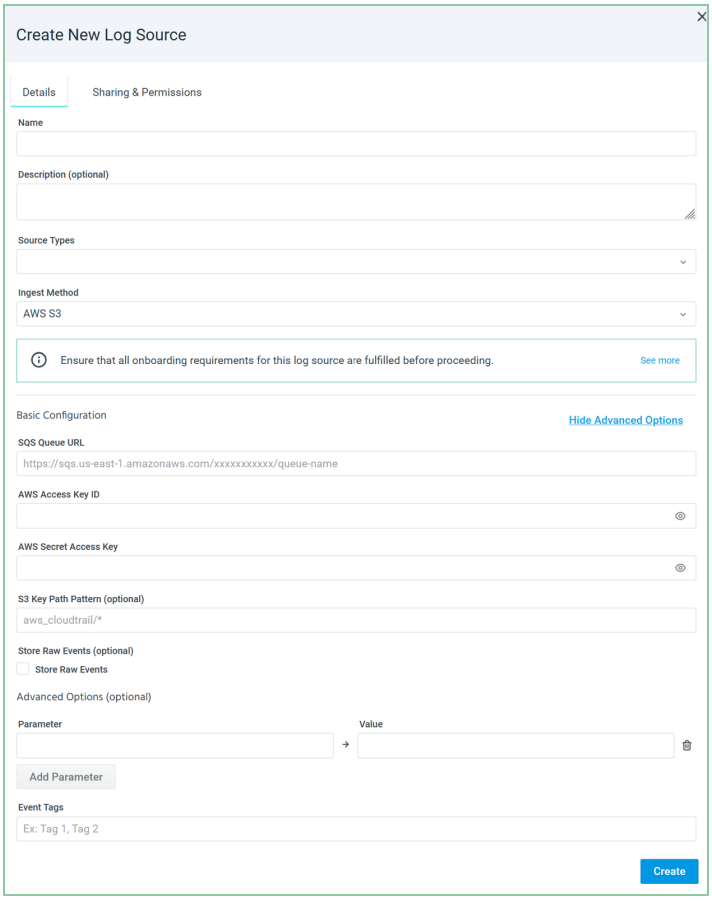
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Oracle IAM Replication as new log source



On the Anomali platform, add Oracle IAM Replication as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `oracle_iam_replication/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"oracle_iam_replication"` is correct, however `"Oracle IAM Replication"` is incorrect.

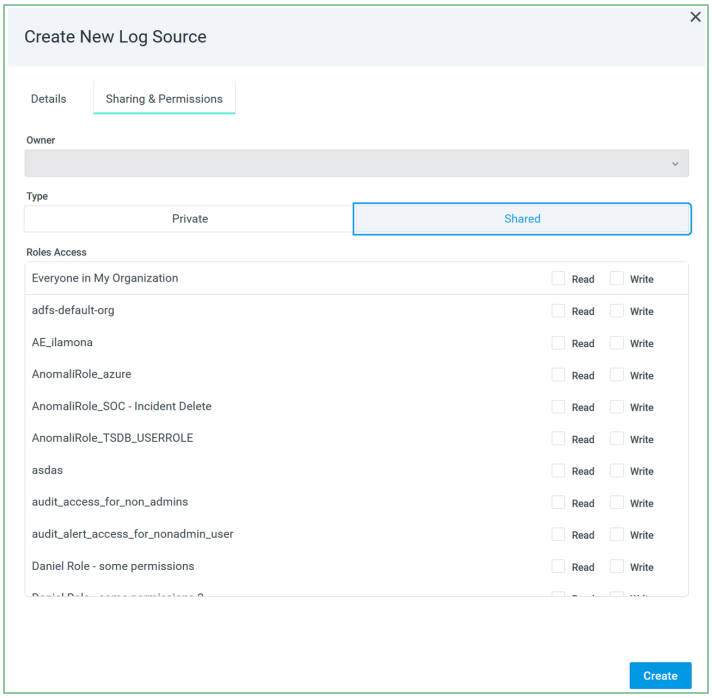
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Palo Alto Networks Firewall

Anomali supports the ingestion of Palo Alto Networks Firewall logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

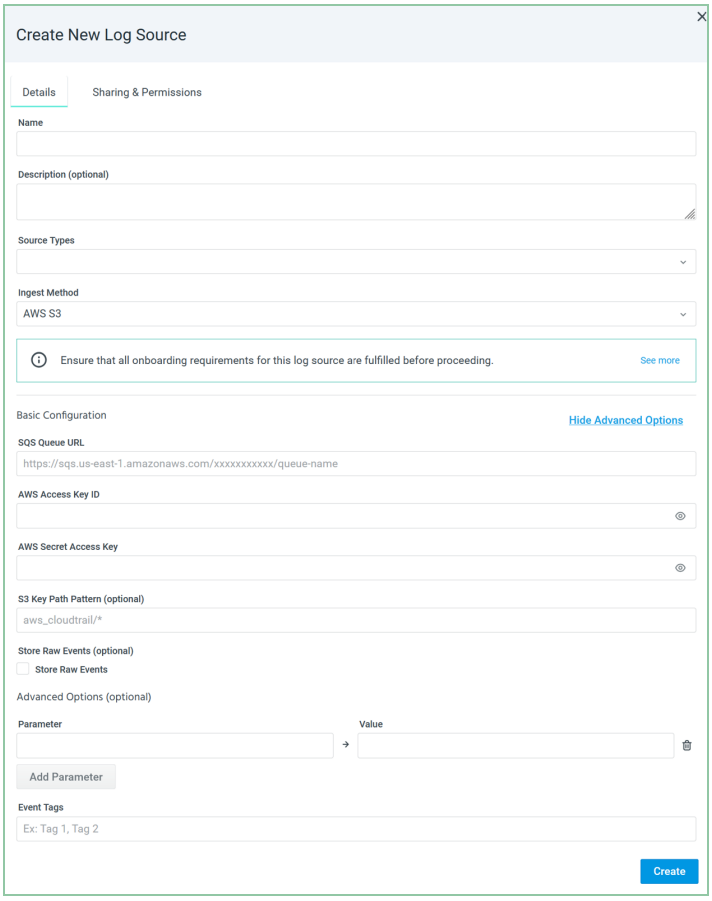
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add PAN as new log source



On the Anomali platform, add PAN as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `pan_fw/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"pan_fw"` is correct, however `"pan fw"` is incorrect.

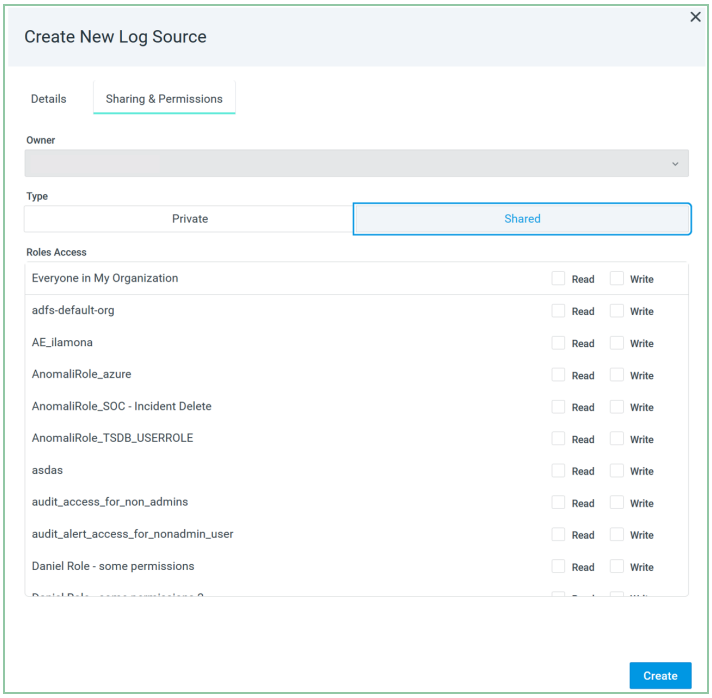
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Proofpoint

Anomali supports the ingestion of Proofpoint logs through the Proofpoint SIEM API.

REST API

You can use your existing API token or create a new token to add a new log source in the Anomali platform.

Onboarding steps

Step 1: Create API token and Service Principal

1. Sign into the Proofpoint console.
2. Navigate to **Settings**.
3. Click **New token** to generate a token.
4. Securely store the Token Service Principal and the Token Secret for the subsequent steps.

Step 2: Add Proofpoint as new log source

To add Proofpoint as a new log source on the Anomali platform:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select **Proofpoint** as the source type.
6. Select **API** as the ingestion method.
7. Select API as the ingest method.
8. Provide the Basic Configuration details:
    a. **Service Principal**: Enter the Token Service Principal of the new token you created in "Step 1: Create API token and Service Principal" above.

b. **API Secret**: Enter the API secret of the new token you created in "Step 1: Create API token and Service Principal" on the previous page.

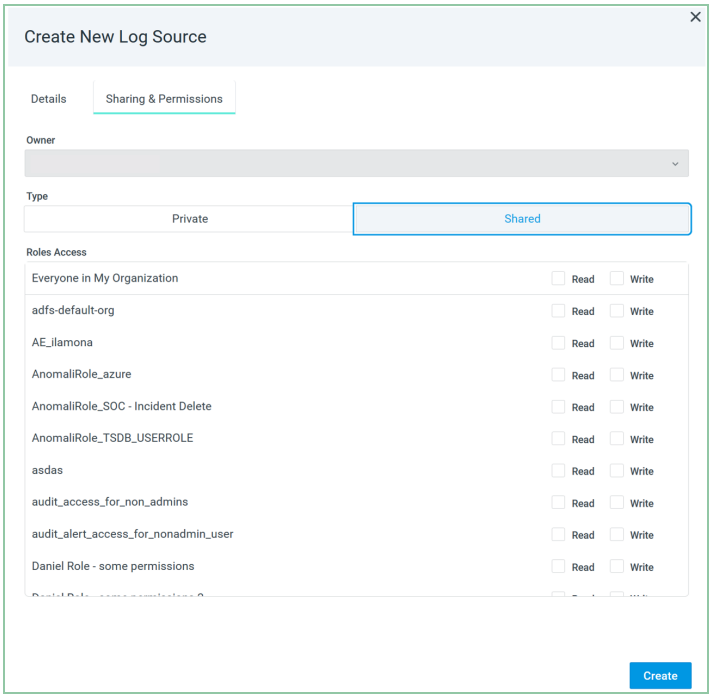
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 3: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.

2. Type: Select the type of permission assigned to the view:

a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.

b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 4: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 5: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

PagerDuty

Anomali supports the ingestion of PagerDuty logs through the PagerDuty REST API v2.

REST API

You can use your existing API token or create a new token to add a new log source in the Anomali platform.

Onboarding steps

Step 1: Create API token

1. Sign into the PagerDuty console.
2. Navigate to **Integrations** > **Developer Tools** > **API Access Keys**.
3. Click **Create New API Key**.
4. Enter a description for the token, for example, `Anomali API token`. Securely store the token value for the subsequent steps.
5. Click **Create Key**.

For more information, see PagerDuty's guide to Create API Access Keys.

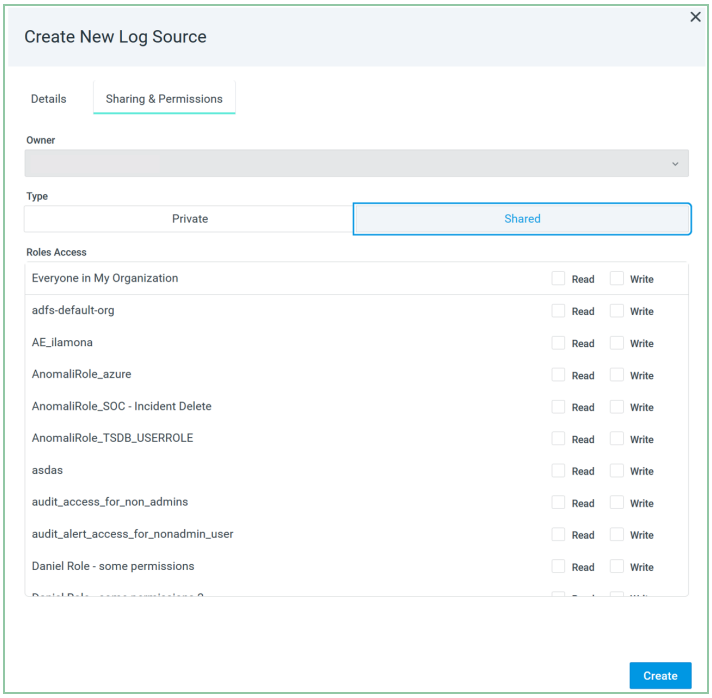
Step 2: Add PagerDuty as a new log source

To add PagerDuty as a new log source on the Anomali platform:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select **PagerDuty** as the source type.
6. Select **API** as the ingestion method.
7. Select API as the ingest method.

8. Provide the Basic Configuration details:
   a. **Token**: Enter your existing token ID or the new token you created in "Step 1: Create API token" on the previous page.
   b. **PagerDuty domain**: Enter your PagerDuty domain name.
   c. (Optional) **Enabled actions**: Provide all the PagerDuty enabled actions you would like to ingest into Anomali.
   d. (Optional) **Enabled actor ID**: Provide the enabled actor ID.
   e. (Optional) **Enabled actor type**: Provide the enabled actor type.
   f. (Optional) **Enabled method type**: Provide the enabled method type.
   g. (Optional) **Enabled root resource types**: Provide all the enabled root resource types.
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:
   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.
   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.
10. Click **Save** to add the log source.

Step 3: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 4: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 5: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

IBM QRadar

Anomali supports the ingestion of QRadar logs. The following article explains the steps you must complete to ingest QRadar logs into Anomali.

Onboarding steps

Prerequisites

You must have QRadar administrator privileges to create authorized service tokens.

Step 1: Create token

Create an admin token using IBM's guide to Creating authorized service tokens.

Step 2: Add QRadar as new log source

To add QRadar as a new log source on the Anomali platform:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select **QRadar** as the source type.
6. Select **API** as the ingestion method.
7. Select API as the ingest method.
8. Provide the Basic Configuration details:
    a. **Token**: Enter the authentication token for the connection to the QRadar instance.
    b. **QRadar API Version**: Enter the API version number. Version 12.0, 11.0, 10.0, and 8.0 are supported. The default is 12.0.
    c. **QRadar URL**: Enter the IP address or FQDN part of the URL for the QRadar instance.
    d. **QRadar queries**: Enter the access key to authenticate requests.

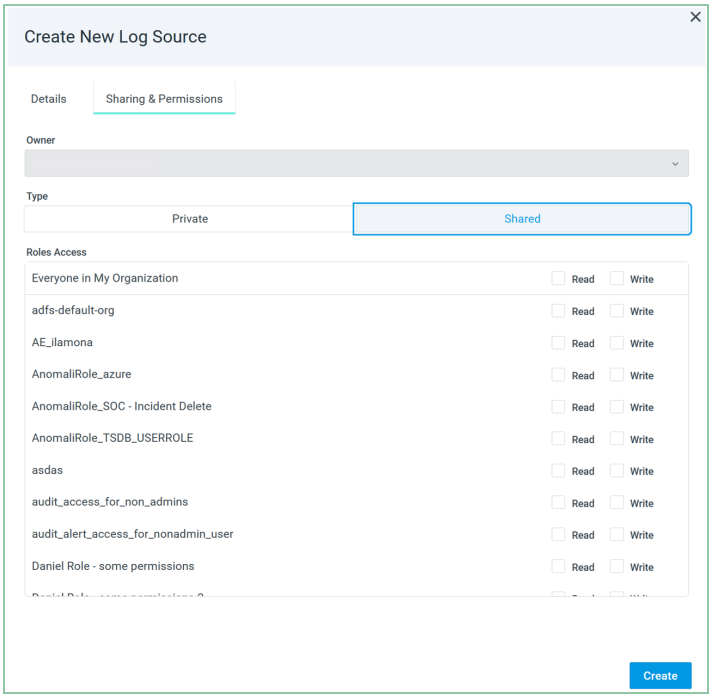
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

    a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

    b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 3: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.

2. Type: Select the type of permission assigned to the view:

    a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.

b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 4: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 5: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

PRTG

Anomali supports the ingestion of PRTG logs. The following article explains the steps you must complete to ingest PRTG logs into Anomali.

API call

Prerequisites

You must have admin privileges to create API keys.

Step 1: Create API key

Create an admin token using PRTG's guide to Creating API Keys.

Step 2: Add PRTG as new log source

To add PRTG as a new log source on the Anomali platform:

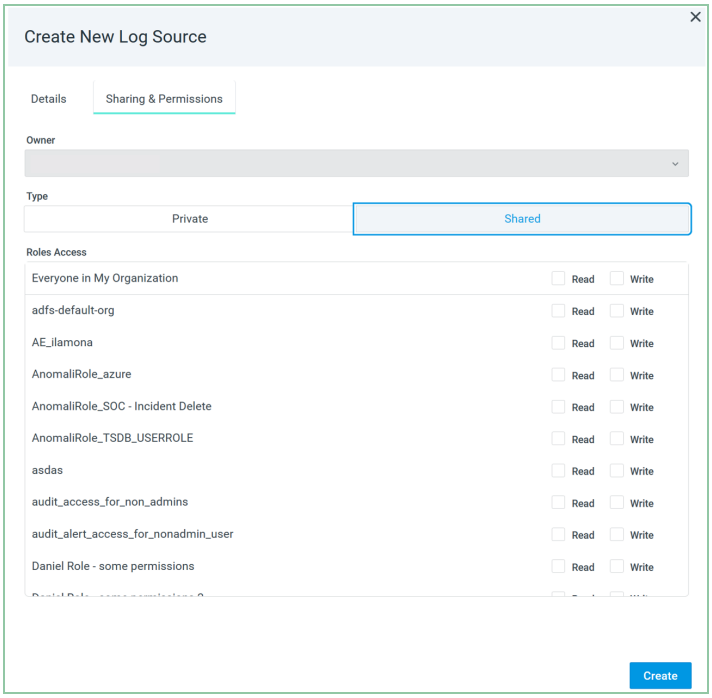
1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select **PRTG** as the source type.
6. Select **API** as the ingestion method.
7. Select API as the ingest method.
8. Provide the Basic Configuration details:
   a. **Token**: Enter the authentication token.
   b. **Username**: Enter the username.
   c. **PRTG domain**: Enter the PRTG IP address or FQDN.
   d. **Content types**: Enter all the content types which you would like to ingest into Anomali.
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 3: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.

2. Type: Select the type of permission assigned to the view:

   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.

   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that

role. You can also assign read or write permissions to everyone in your organization.

Step 4: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 5: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

AWS S3

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

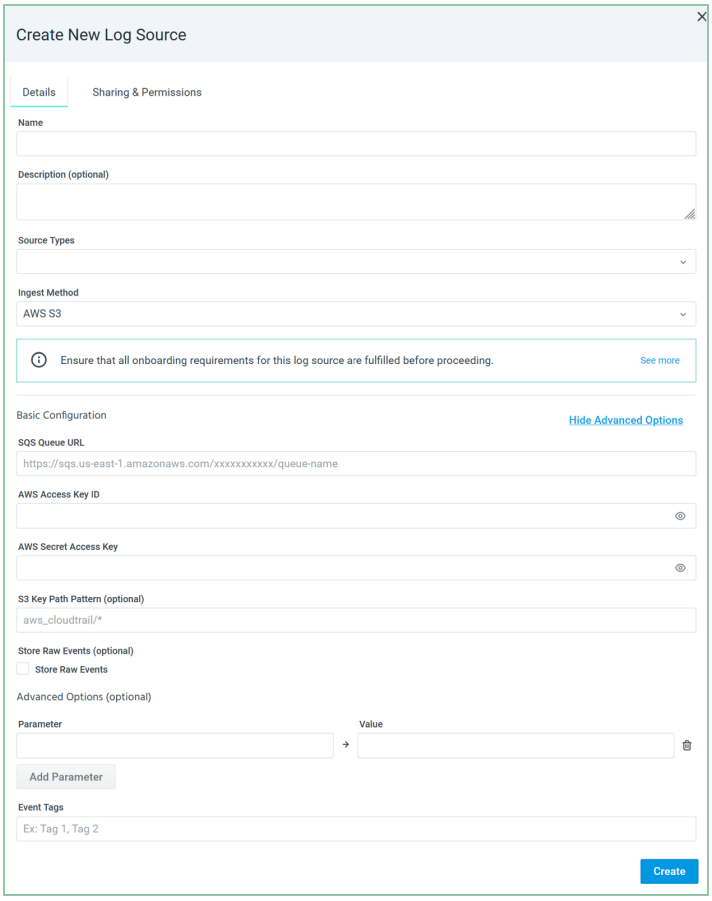
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add PRTG as new log source



On the Anomali platform, add PRTG as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `prtg/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"prtg"` or `"prtg_sourcetype"` are correct, however `"prtg sourcetype"` is incorrect.

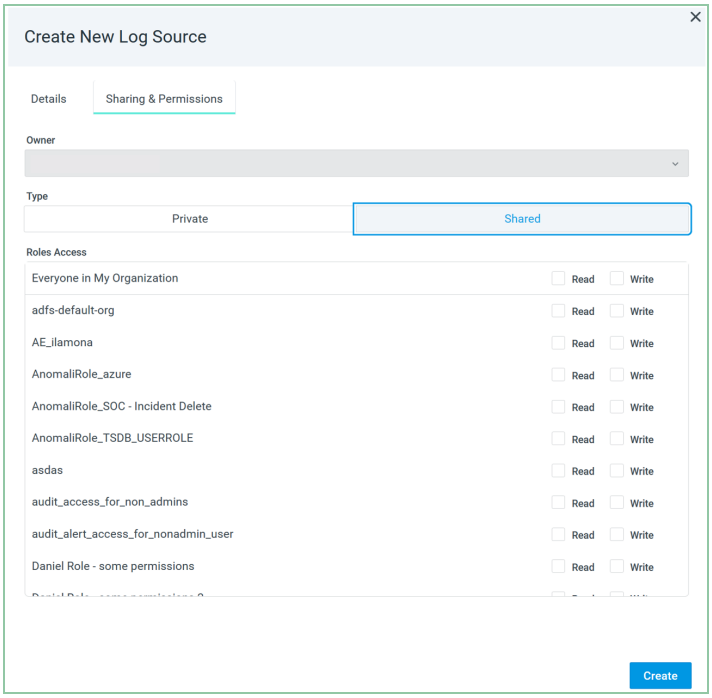
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Secure Relay

Anomali supports the ingestion of Secure Relay logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

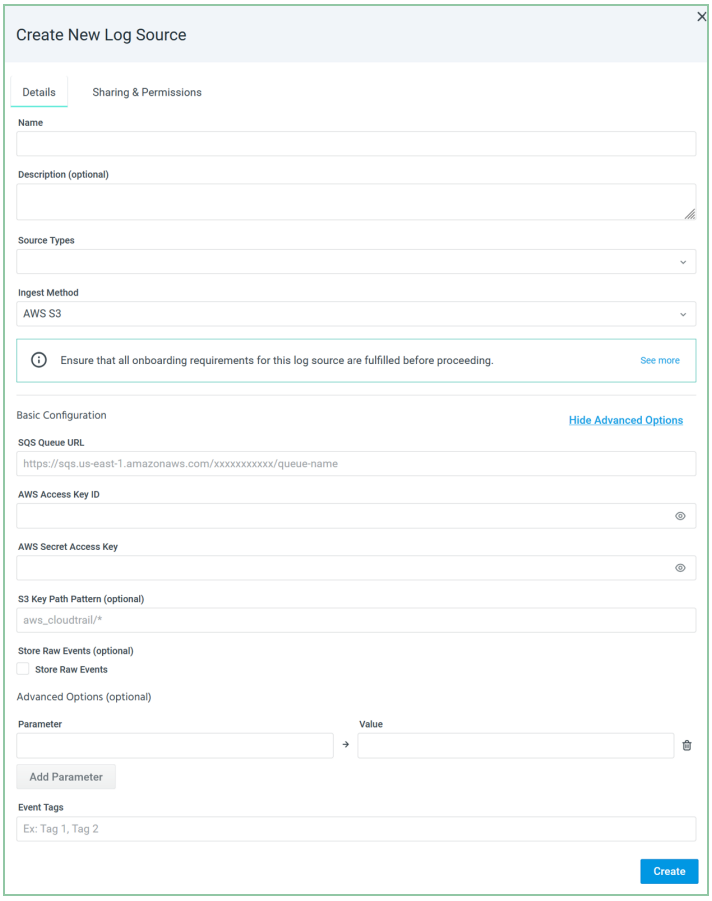
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Secure Relay as new log source



On the Anomali platform, add Secure Relay as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `secure_relay/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"secure_relay"` is correct, however `"Secure Relay"` is incorrect.

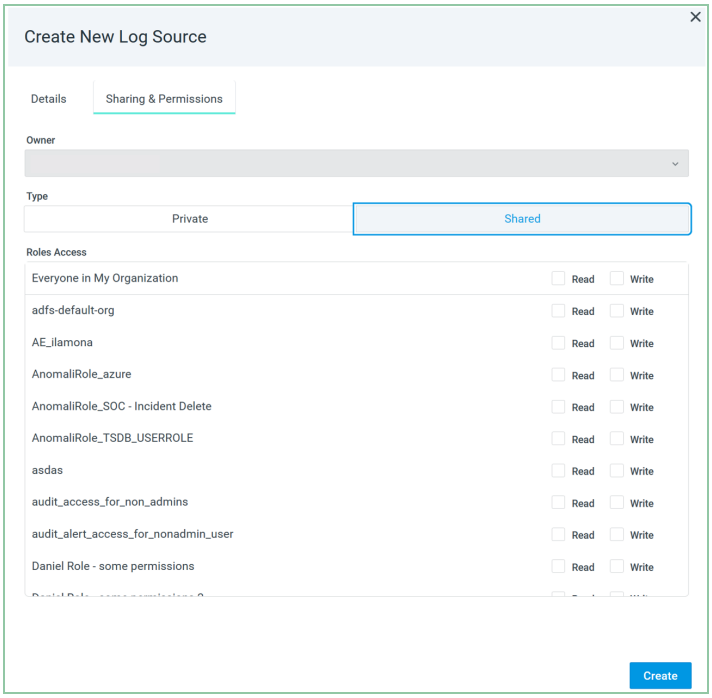
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

ServiceNow

Anomali supports the ingestion of ServiceNow logs through the inbound ServiceNow "REST API" below or "AWS S3" on page 942.

REST API

Onboarding Steps

Step 1: Create authentication credentials on ServiceNow

Create a ServiceNow user account with Basic Authentication for inbound REST API calls to ServiceNow that will be used by Anomali to ingest logs from your ServiceNow instance. Typically, this involves the steps outlined here. Anomali recommends referring to your ServiceNow documentation for instructions pertinent to your ServiceNow release.

1. Go to **User Administration** > **Users**.
2. Create a user with:
   - Username and password
   - Assigned roles to ensure that user will have access to the logs that are to be ingested

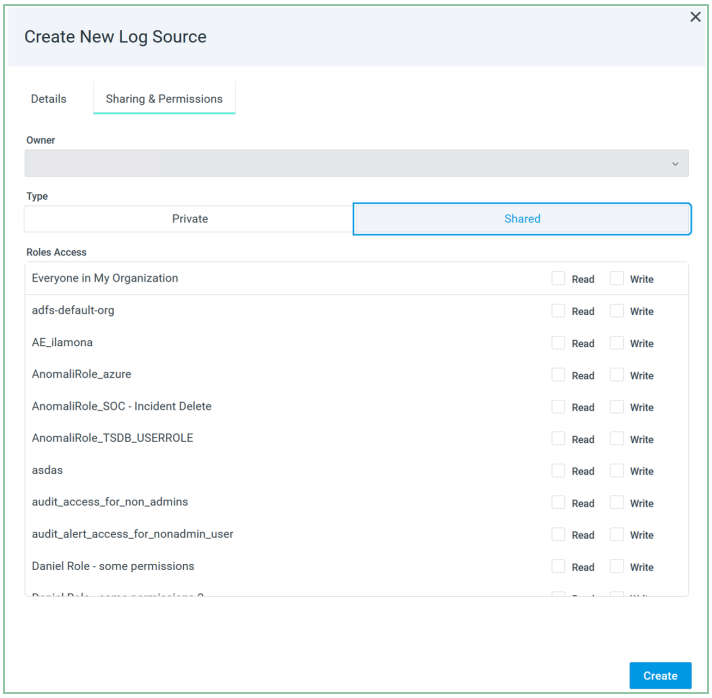
Step 2: Add ServiceNow as new log source on Anomali

To add ServiceNow as a new log source on the Anomali platform:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select **ServiceNow** as the source type.
6. Select **API** as the ingestion method.
7. Select API as the ingest method.

8. Provide the Basic Configuration details:
   a. **Username**: Enter the ServiceNow account username, from "Step 1: Create authentication credentials on ServiceNow" on the previous page.
   b. **Password**: Enter the ServiceNow account password, from "Step 1: Create authentication credentials on ServiceNow" on the previous page.
   c. **ServiceNow instance URL**: Provide the ServiceNow instance URL.
   d. (Optional) **Enabled tables**: Enter the API path to the target table in ServiceNow to which this user has access.
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:
   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.
   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.
10. Click **Save** to add the log source.

Step 3: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 4: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 5: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

AWS S3

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

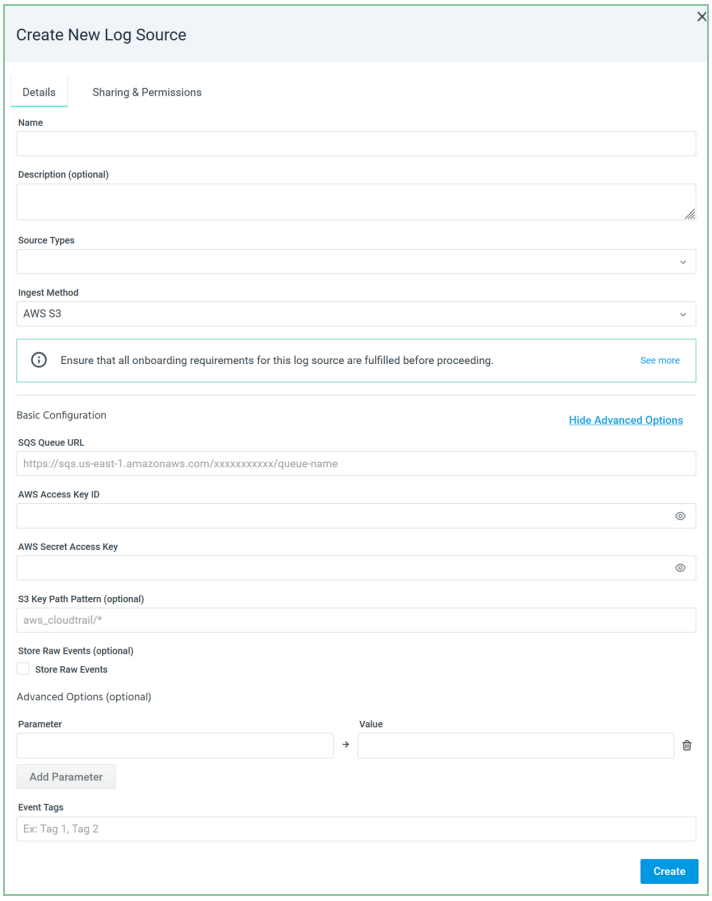
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add ServiceNow as new log source



On the Anomali platform, add ServiceNow as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `servicenow/year=2025/month=03/day=22/events/event_data_logs/`.

- Sourcetype name must not contain any spaces: For example, `"servicenow"` or `"servicenow_sourcetype"` are correct, however `"servicenow sourcetype"` is incorrect.

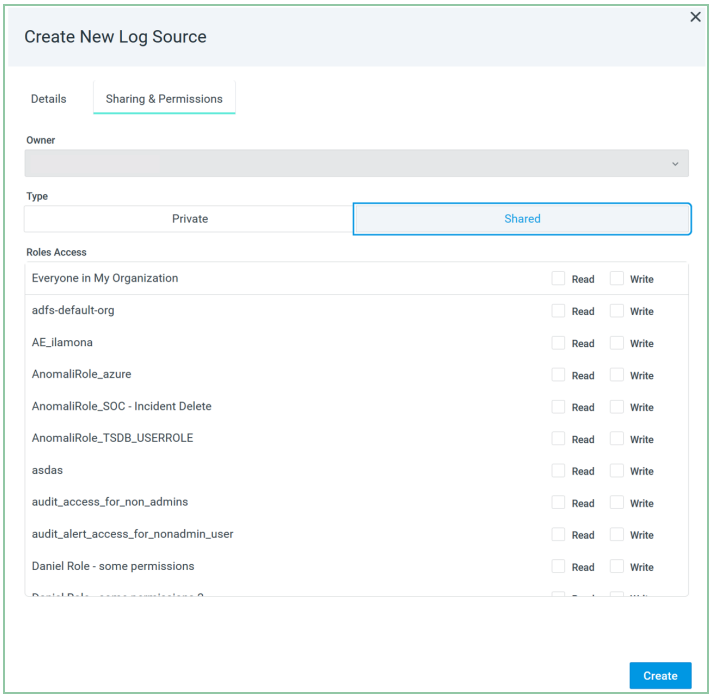
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Sumo Logic

Anomali Security Analytics can ingest event log data from Sumo Logic. The following article explains the steps you must complete to ingest Sumo Logic logs into Anomali.

API call

Step 1: Create Access Keys

Create an admin access key using Sumo Logic's guide to Creating an Access Key.

Step 2: Add Sumo Logic as new log source

To add Sumo Logic as a new log source on the Anomali platform:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select **Sumo Logic** as the source type.
6. Select **API** as the ingestion method.
7. Select API as the ingest method.
8. Provide the Basic Configuration details:
    a. **Access ID**: Enter the Access ID configured in your Sumo Logic instance.
    b. **Access Key**: Enter the access key corresponding to the access ID.
    c. **Deployment Region**: Select the applicable deployment region. Based on your selection, Sumo Logic determines the API and collection endpoints.
    d. **Search Query**: Provide a Sumo Logic search query. See "Sumo Logic " above for examples.
    e. (Optional) **Ingestion Interval**: Defines a time window, in minutes, hours, days between API requests, for events collected from Sumo Logic.

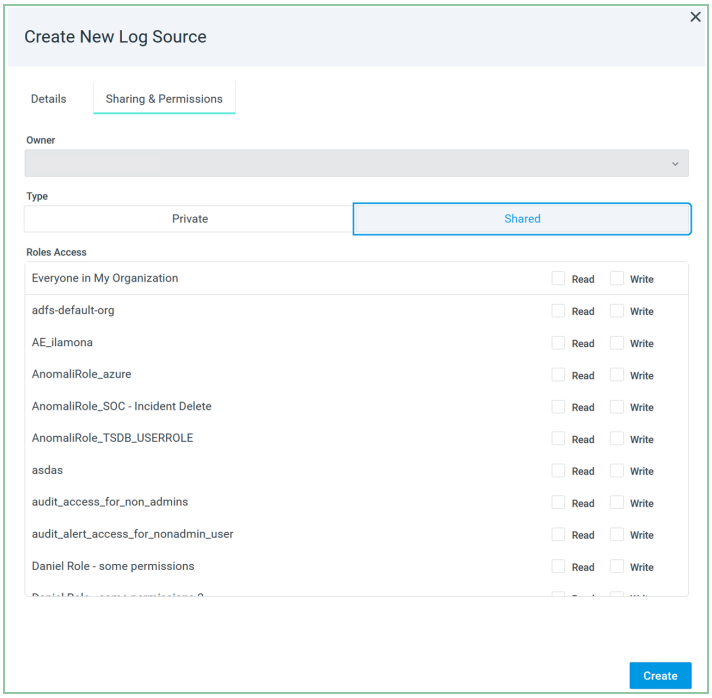
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

    a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

    b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 3: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.

2. Type: Select the type of permission assigned to the view:

    a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.

b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 4: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 5: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

AWS S3

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

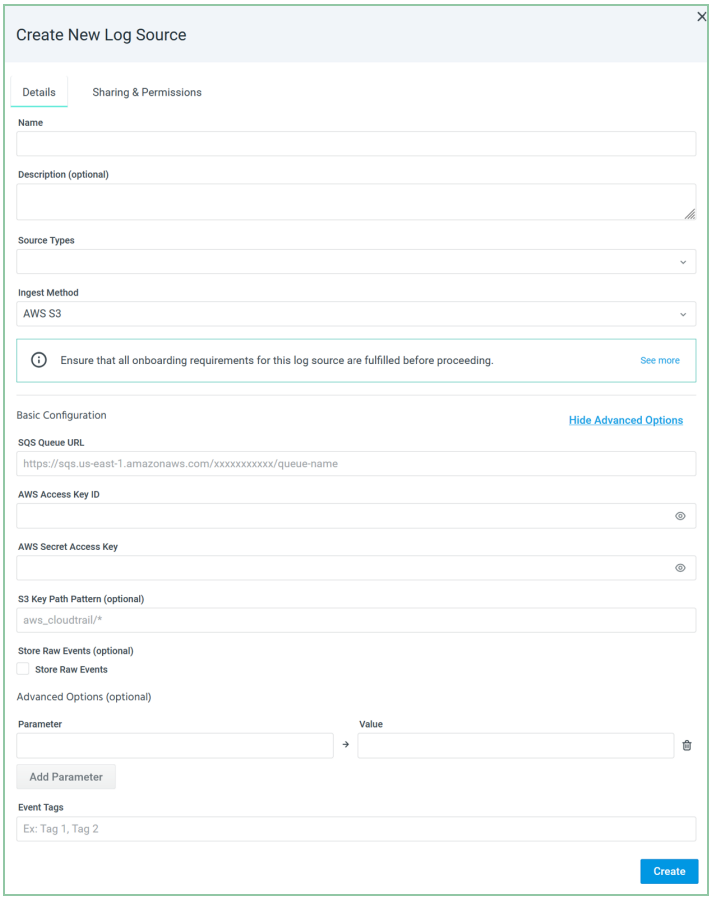
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Sumo Logic as new log source



On the Anomali platform, add Sumo Logic as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `sumo_logic/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"sumo_logic"` is correct, however `sumo logic"` is incorrect.

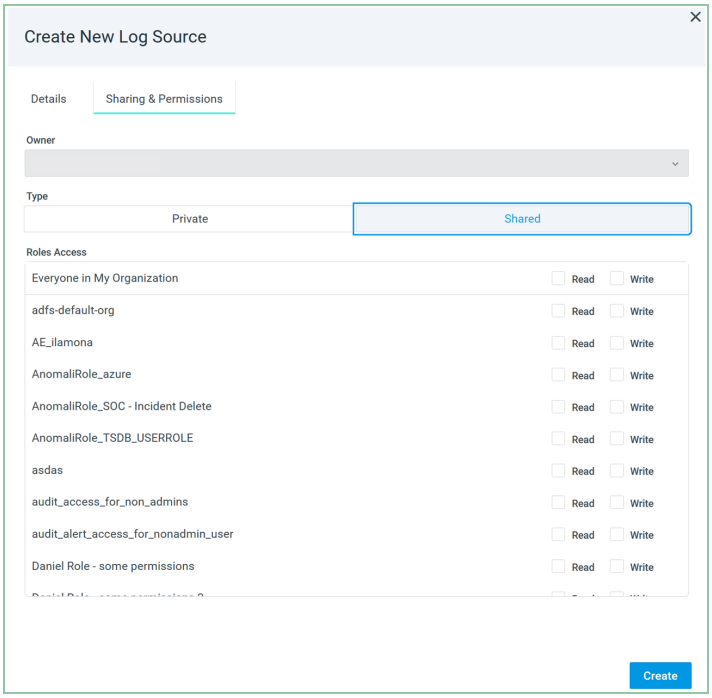
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Suricata

Anomali supports the ingestion of Suricata logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

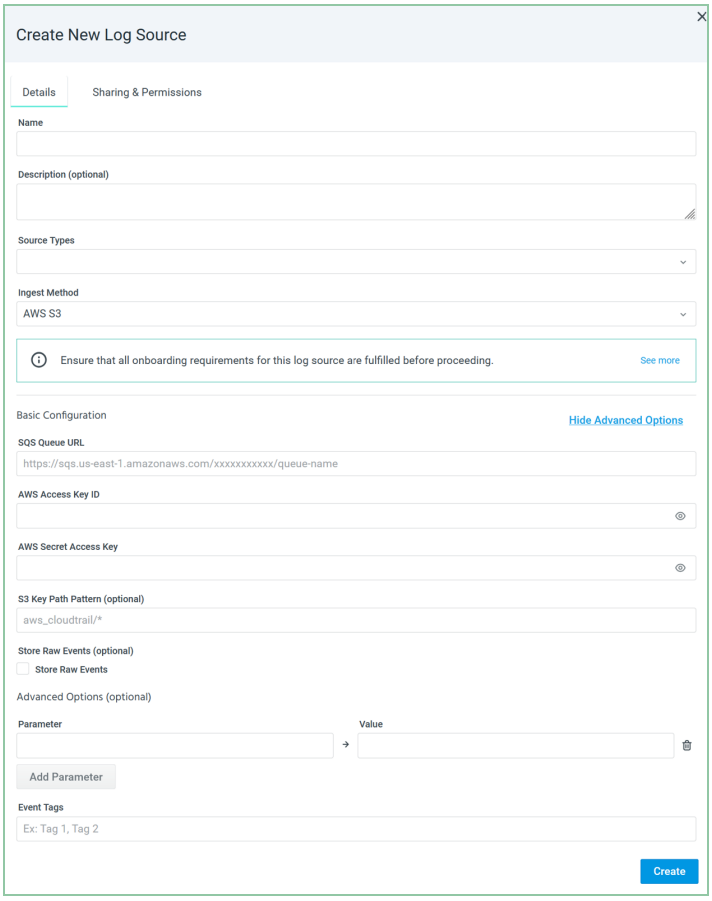
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Suricata as new log source



On the Anomali platform, add Suricata as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `suricata_sourcetype/year=2025/month=03/day=22/events/event_data_logs/`.

- Sourcetype name must not contain any spaces: For example, `suricata` or `"suricata_sourcetype"` are correct, however `"suricata sourcetpye"` is incorrect.

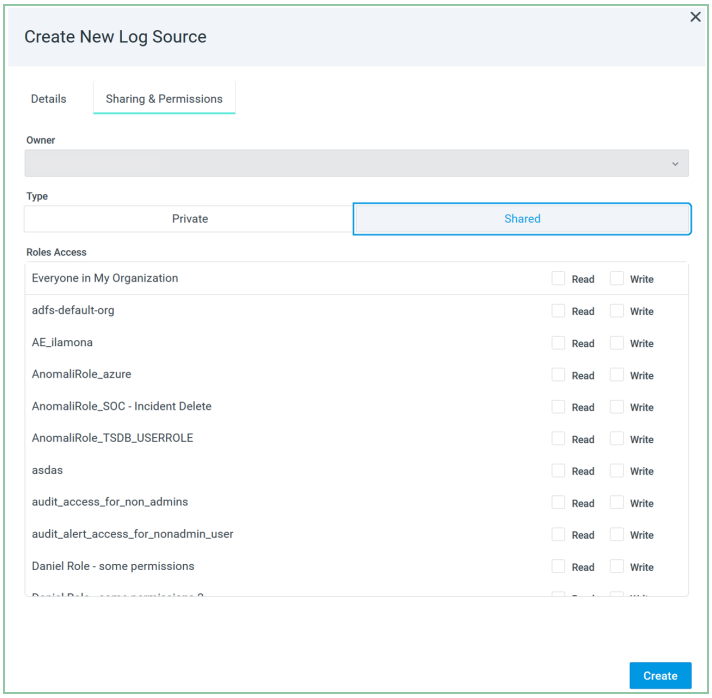
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Tanium HTTP

Anomali supports the ingestion of Tanium HTTP logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

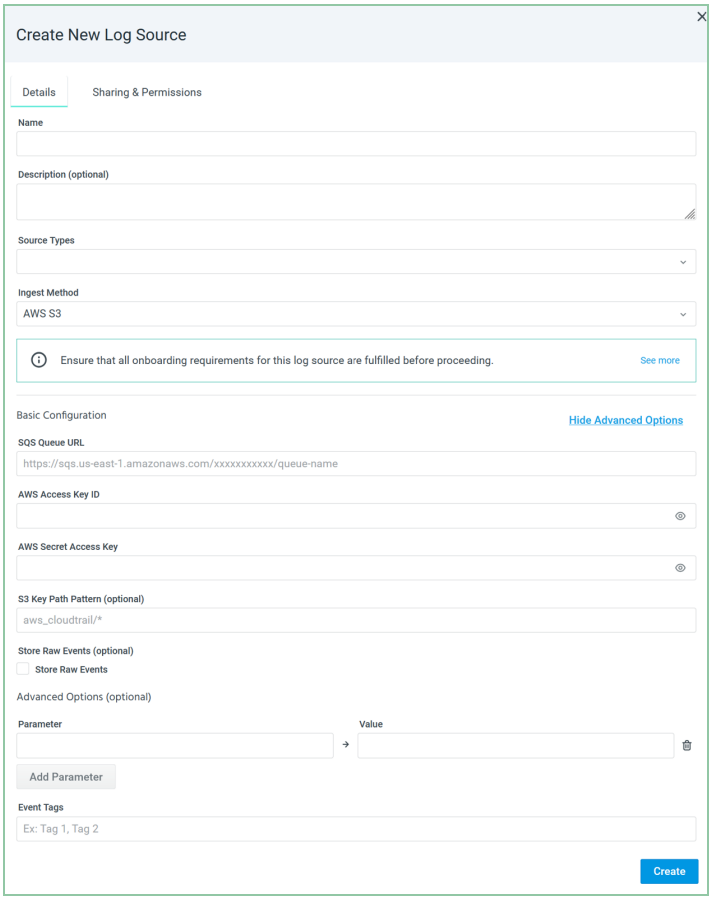
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Tanium HTTP as new log source



On the Anomali platform, add Tanium HTTP as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `tanium_http/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"tanium_http"` is correct, however `"Tanium HTTP"` is incorrect.

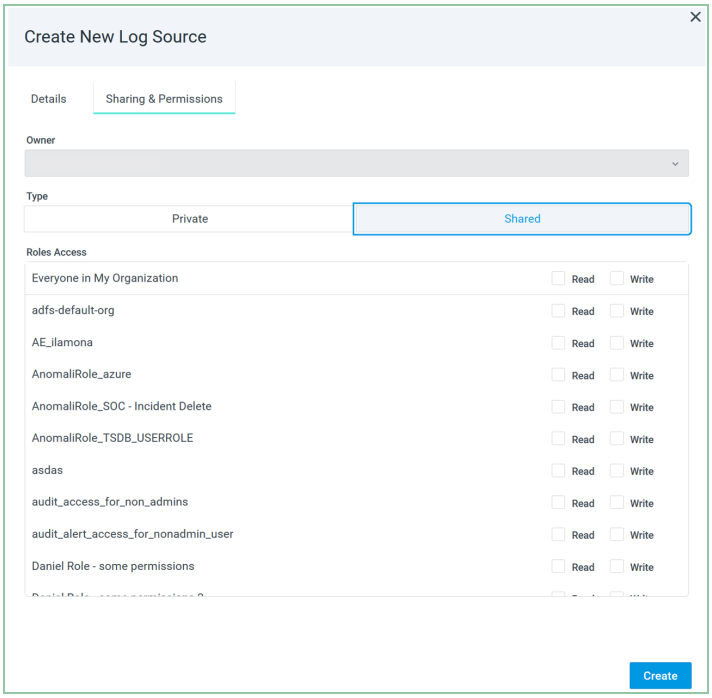
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Thycotic

Anomali supports the ingestion of Thycotic logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

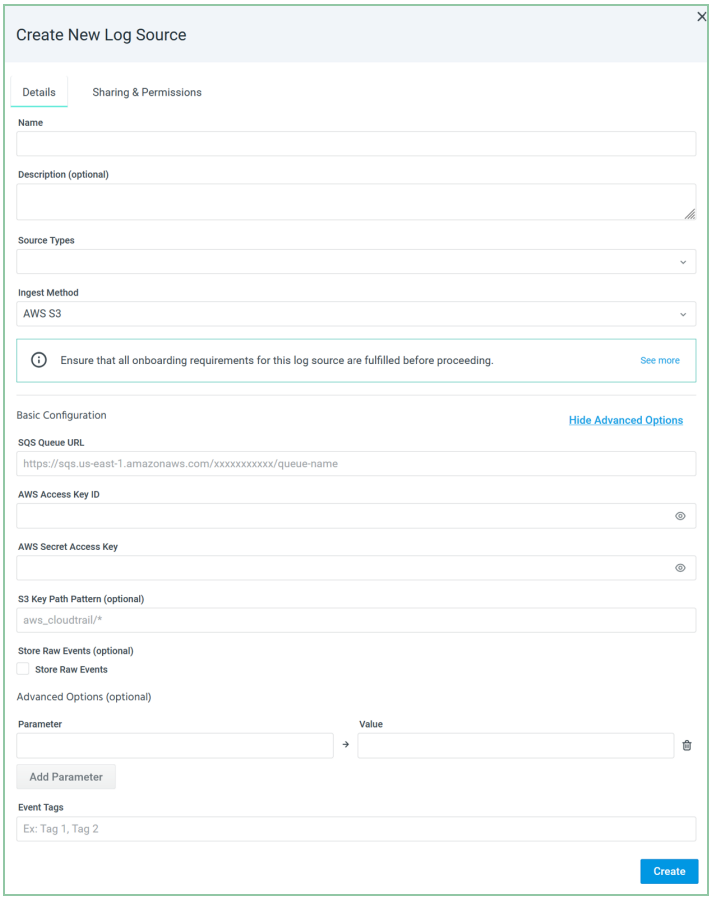
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Thycotic as new log source



On the Anomali platform, add Thycotic as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `thycotic/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"thycotic"` or `"thycotic_sourcetype"` are correct, however `"Thycotic Sourcetype"` is incorrect.

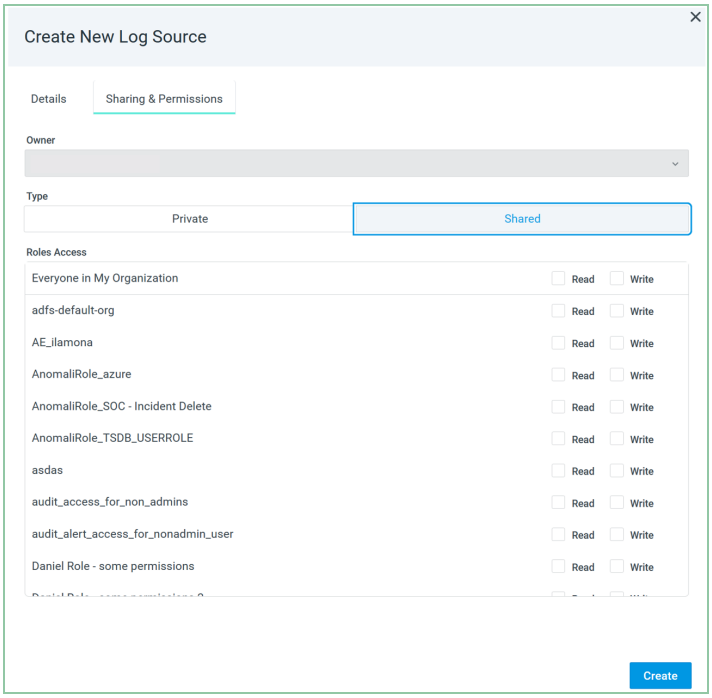
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Windows

Anomali supports the ingestion of Windows logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

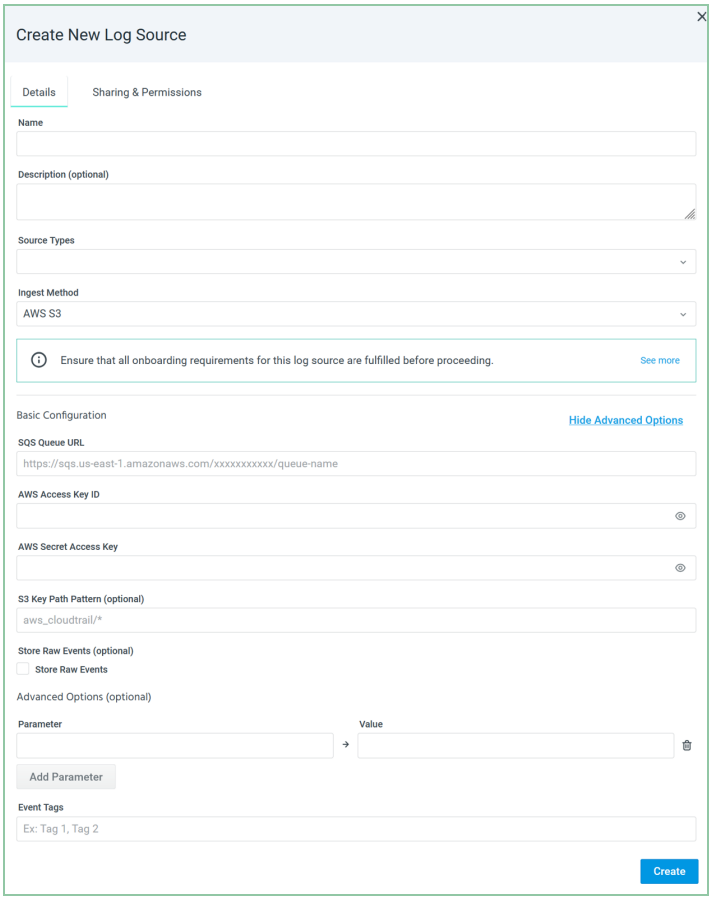
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Windows as new log source



On the Anomali platform, add Windows as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `windows_logs/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"windows_logs"` is correct, however `"windows logs"` is incorrect.

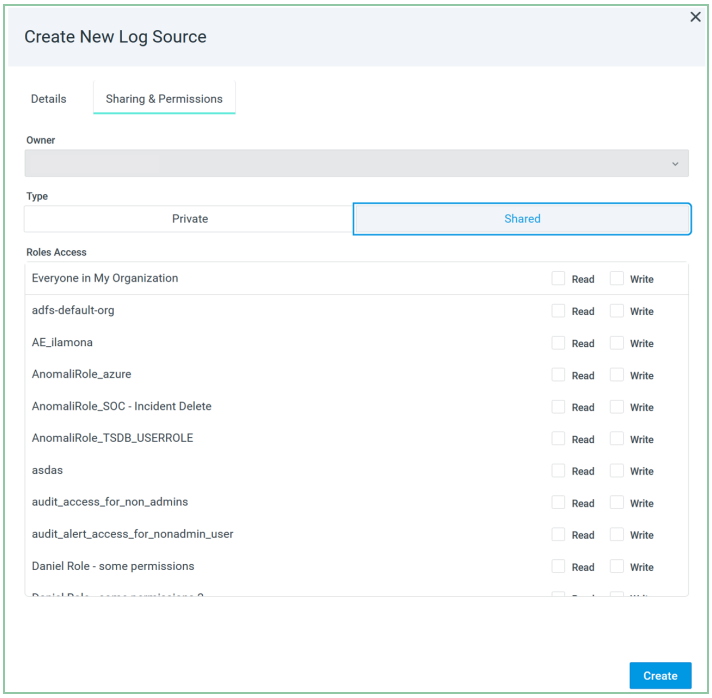
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Windows Event

Anomali supports the ingestion of Windows Event logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

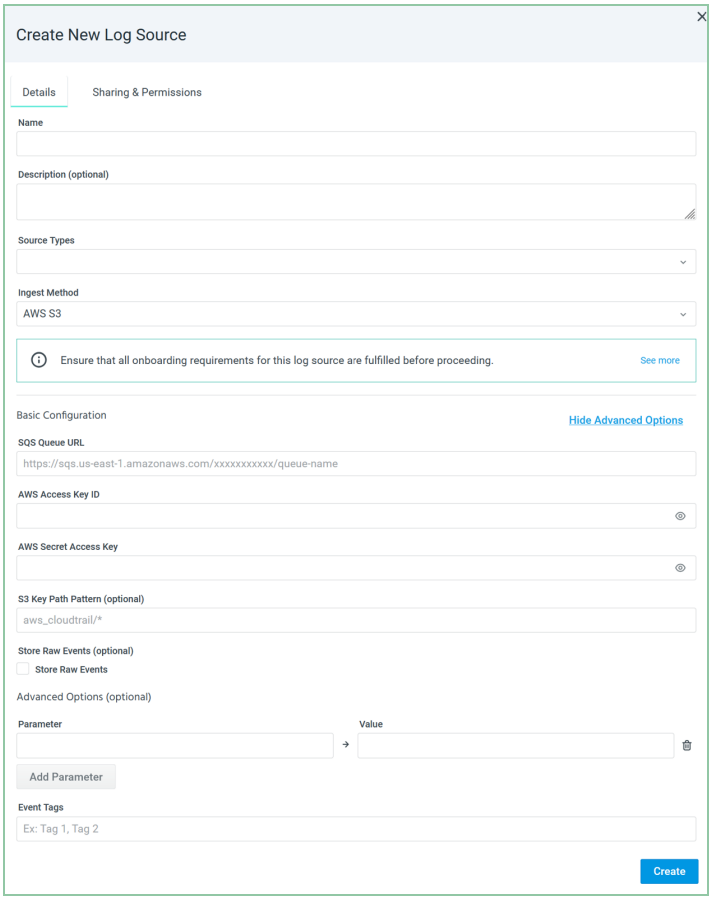
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Windows Event as new log source



On the Anomali platform, add Windows Event as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `windows_event/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"windows_event"` is correct, however `"windows event"` is incorrect.

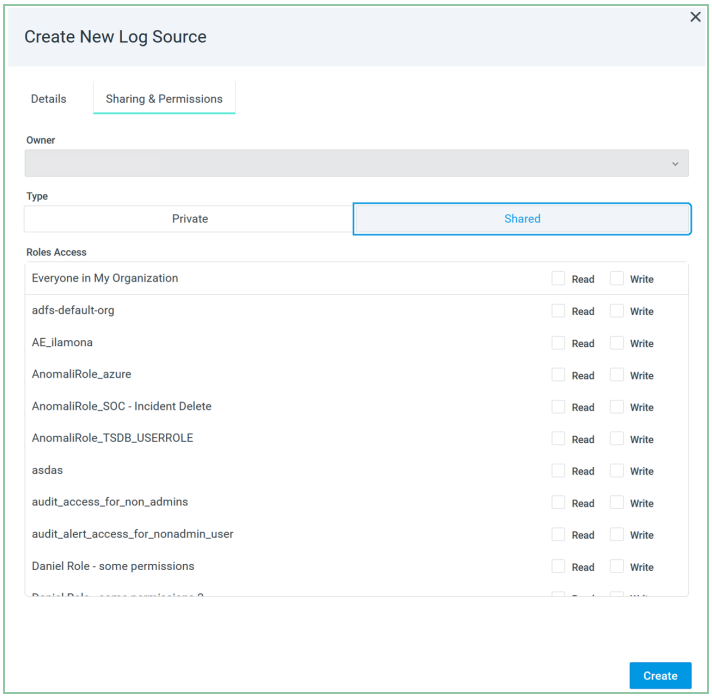
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Wiz

Anomali supports the ingestion of Wiz logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

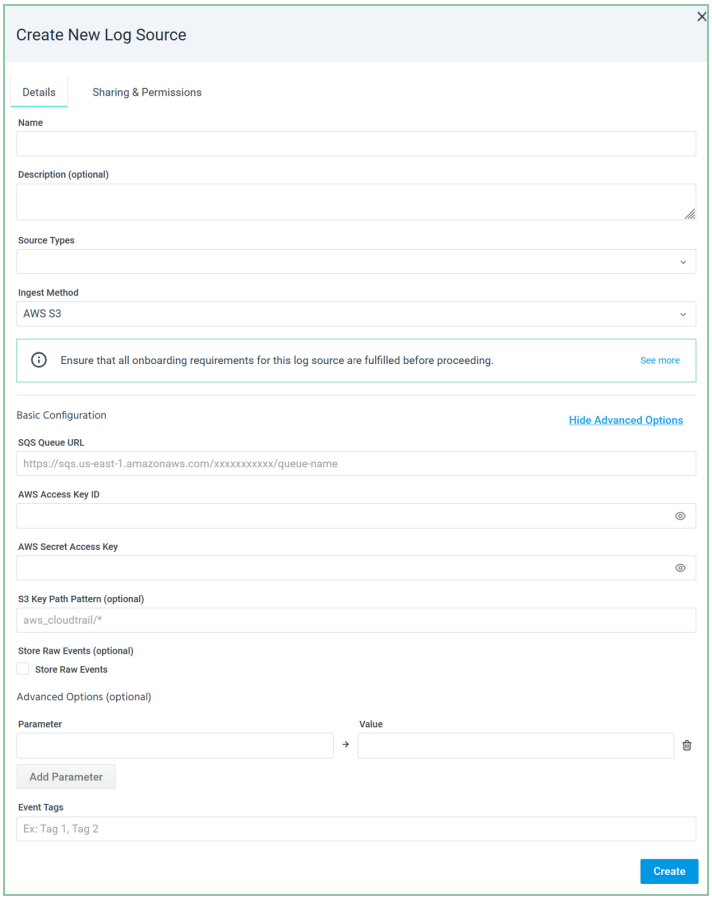
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Wiz as new log source



On the Anomali platform, add Wiz as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `wiz/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"wiz"` or `"wiz_sourcetype"` are correct, however `"Wiz Sourcetype"` is incorrect.

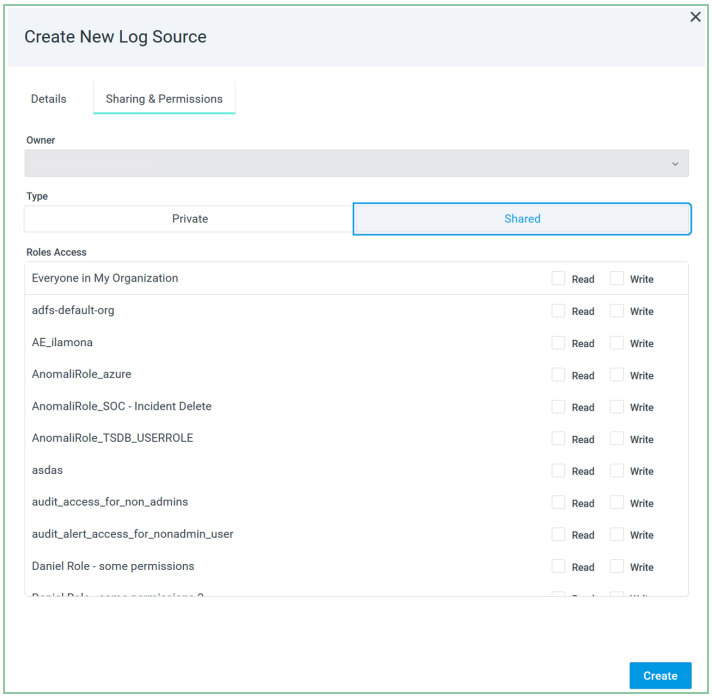
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Zscaler DNS

Anomali supports the ingestion of Zscaler DNS logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

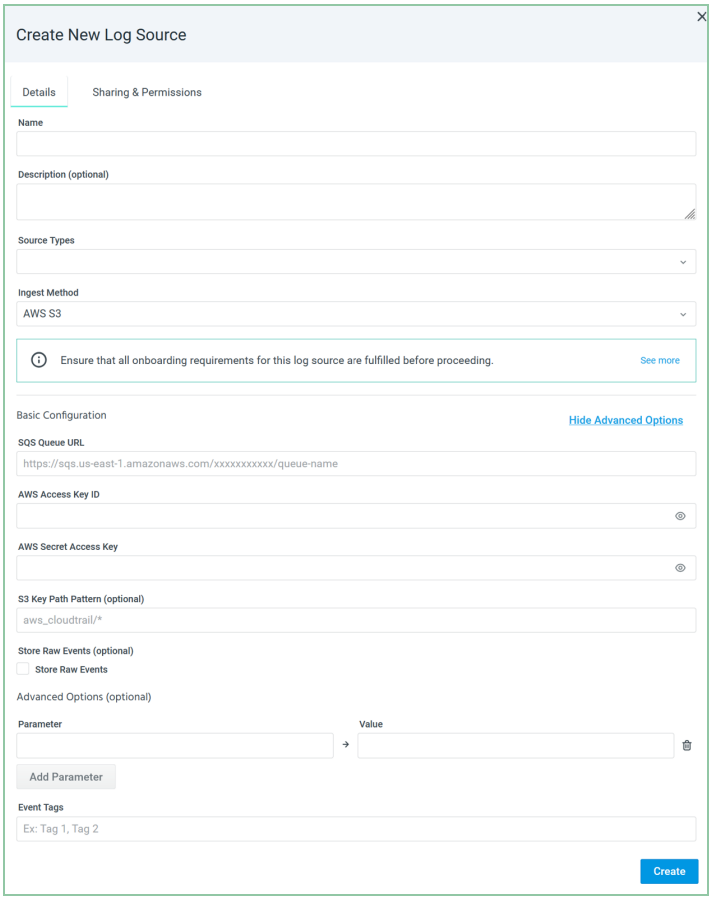
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Zscaler DNS as new log source



On the Anomali platform, add Zscaler DNS as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `zscaler_dns/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"zscaler_dns"` is correct, however `"Zscaler DNS"` is incorrect.

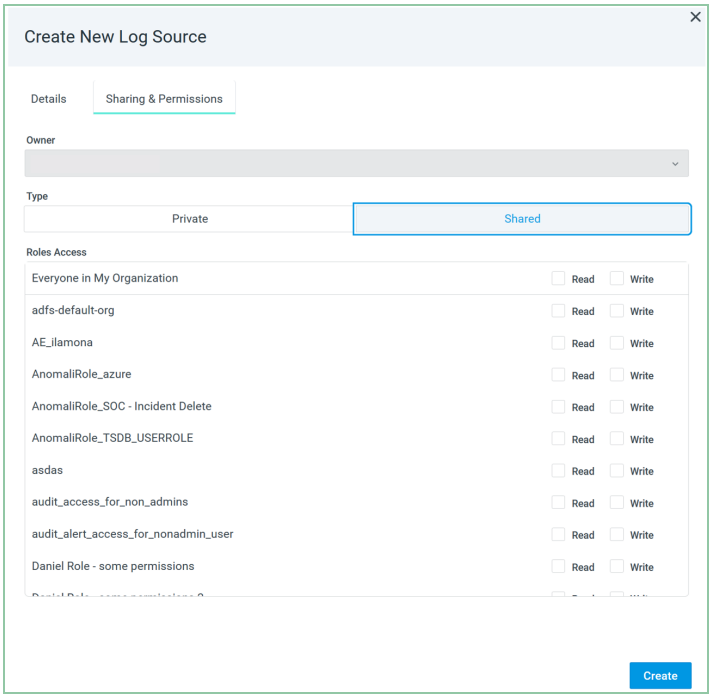
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Zscaler FW

Anomali supports the ingestion of Zscaler FW logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

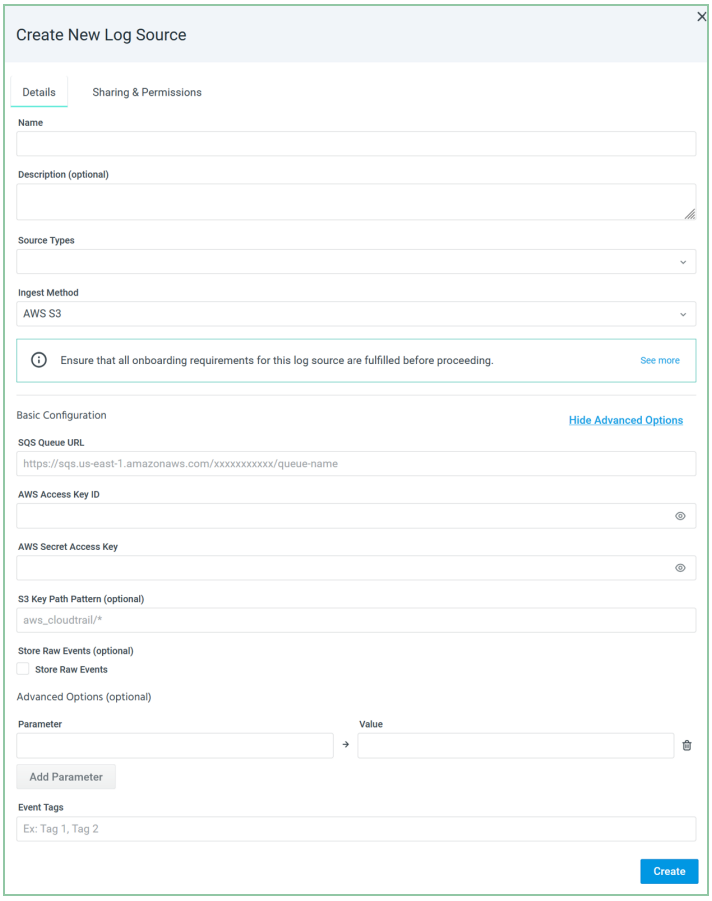
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Zscaler FW as new log source



On the Anomali platform, add Zscaler FW as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `zscaler_fw/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"zscaler_fw"` is correct, however `"Zscaler FW"` is incorrect.

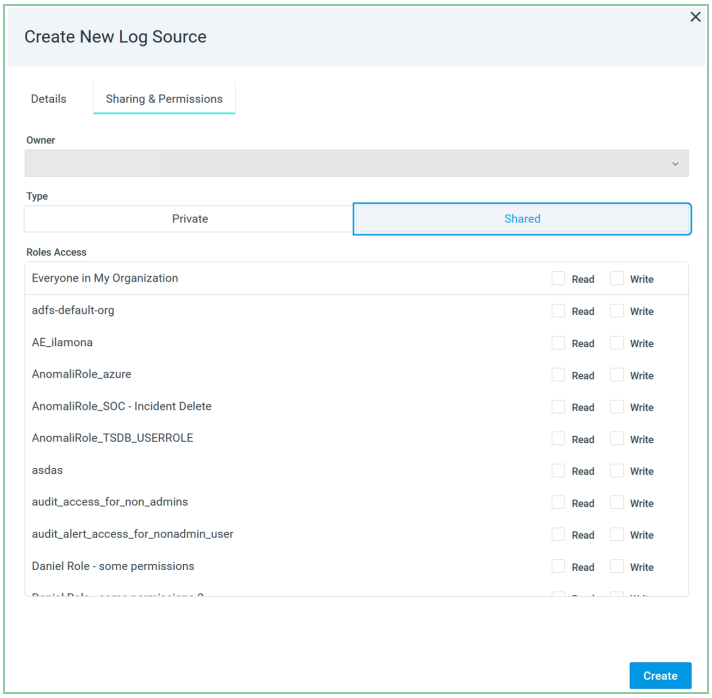
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Zscaler NSS Web

Anomali supports the ingestion of Zscaler NSS Web logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

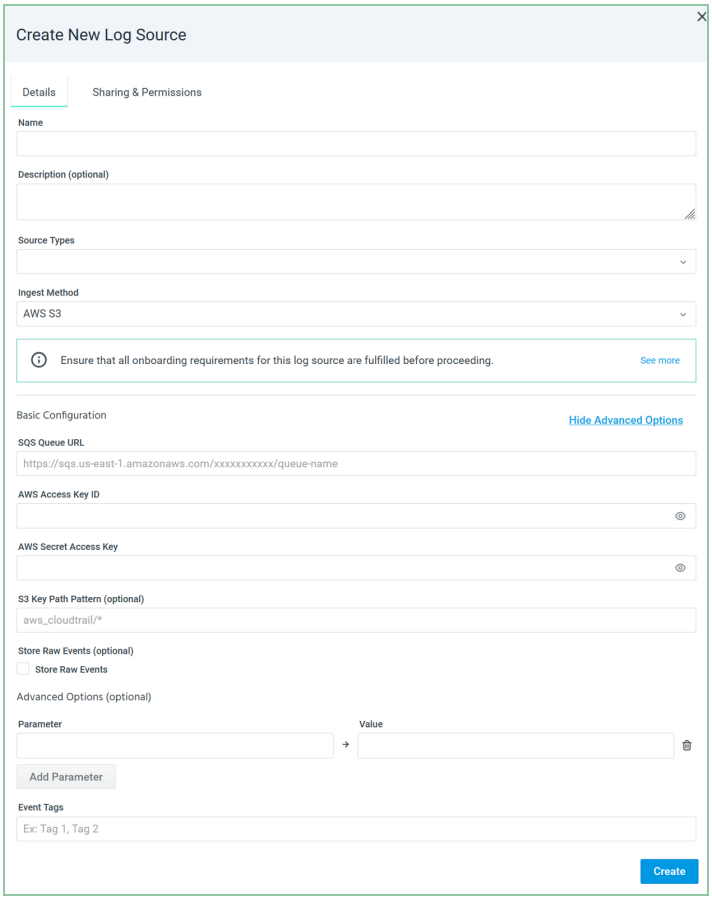
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Zscaler NSS Web as new log source



On the Anomali platform, add Zscaler NSS Web as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `zscaler_nss_web/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"zscaler_nss_web"` is correct, however `"zscaler nss web"` is incorrect.

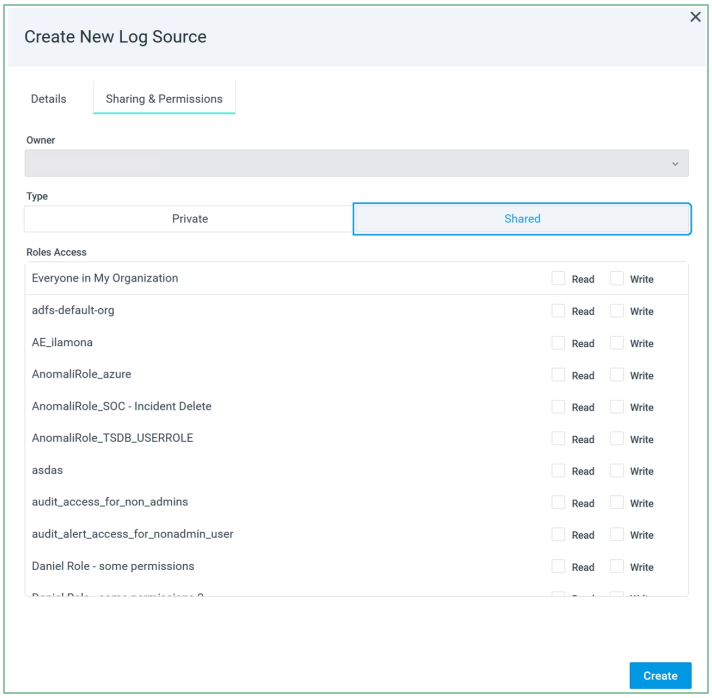
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Zscaler Web

Anomali supports the ingestion of Zscaler Web logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

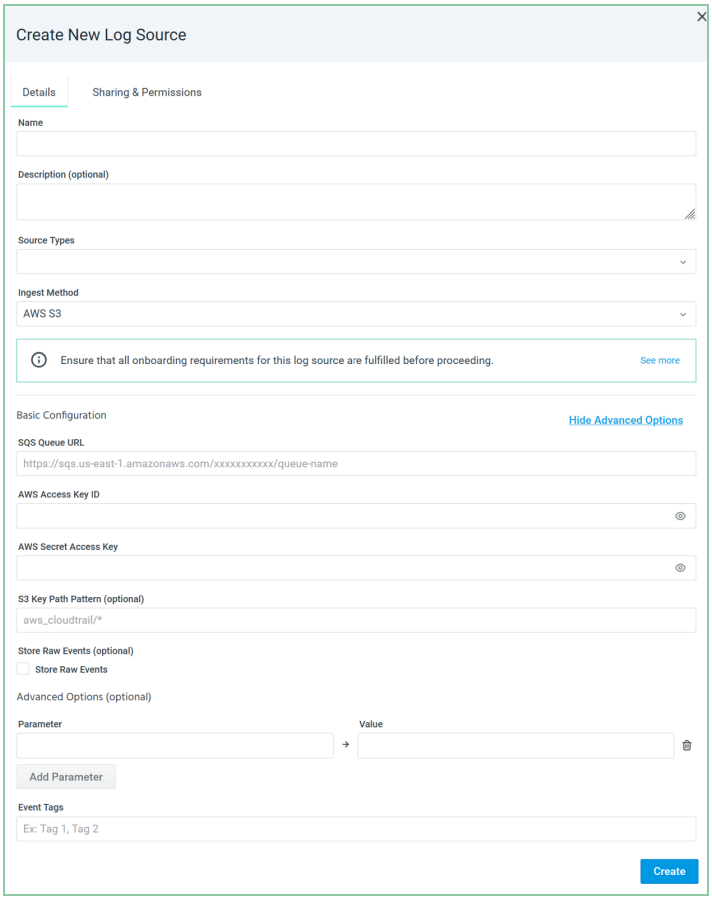
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Zscaler Web as new log source



On the Anomali platform, add Zscaler Web as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `zscaler_web/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"zscaler_web"` or `"zscaler_web"` is correct, however `"zscaler web"` is incorrect.

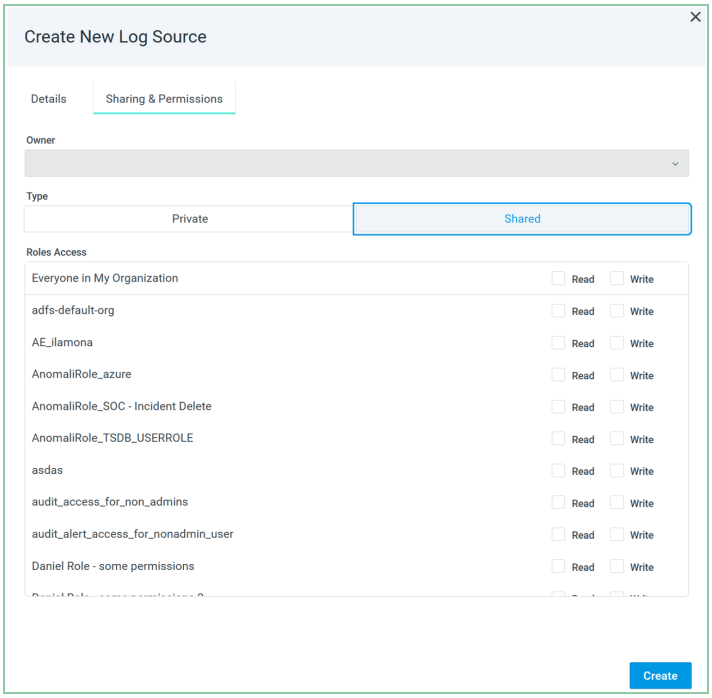
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Zscaler LSS ZPA App

Anomali supports the ingestion of Zscaler Log Streaming Service (LSS) App logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

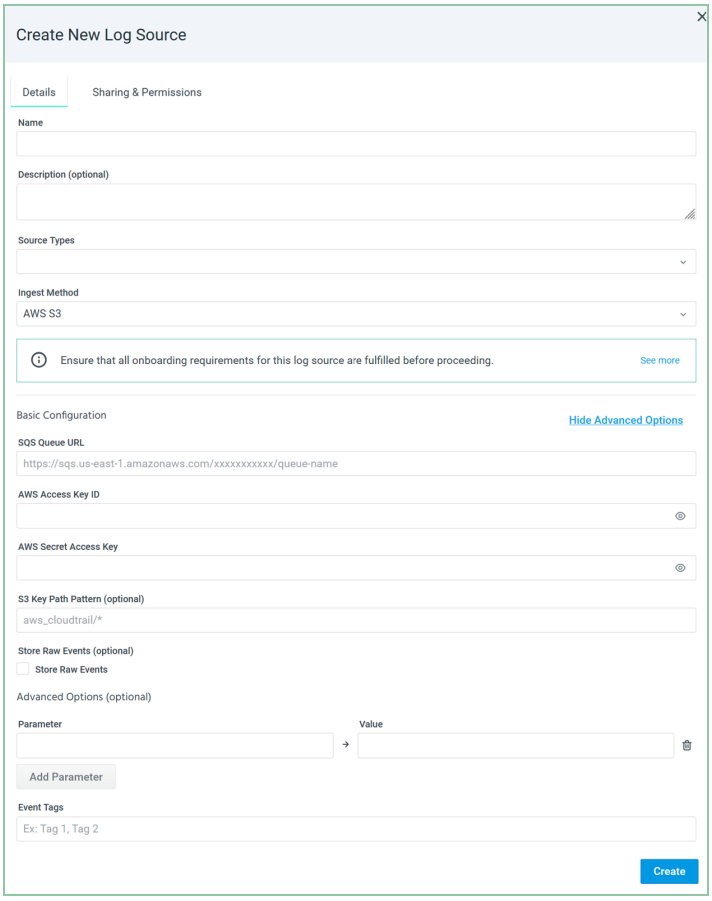
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Zscaler LSS App as new log source



On the Anomali platform, add Zscaler LSS App as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `zscaler_lss_app/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"zscaler_lss_app"` is correct, however `"Zscaler LSS App"` is incorrect.

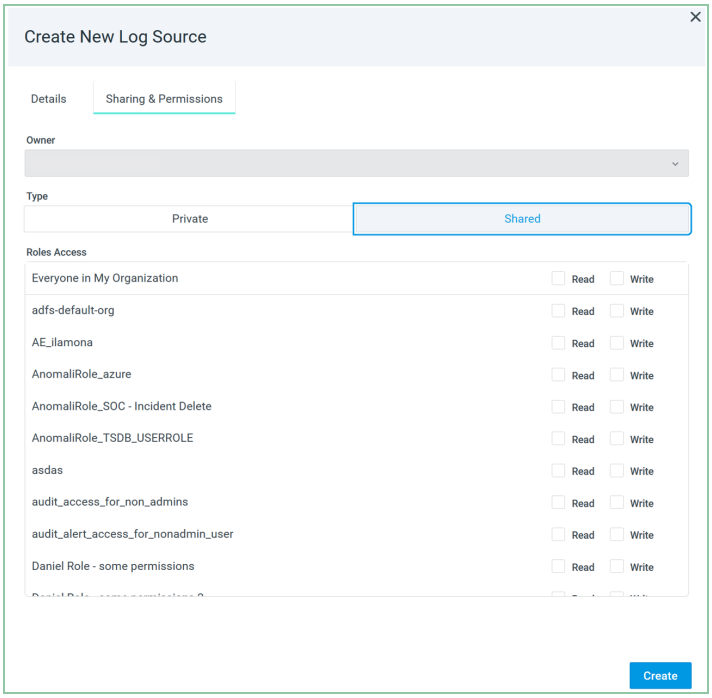
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Zscaler LSS ZPA Auth

Anomali supports the ingestion of Zscaler Log Streaming Service (LSS) Auth logs, assuming that they are stored in AWS S3.

If your logs are already in S3, you can proceed directly to "Step 2: Set up SQS queue" below. If not, Anomali recommends following "Step 1: Ship data to S3 using NXLog" below to use NXLog to first ship the logs to S3. After S3 receives the data, it sends updates to an Amazon SQS queue you designate, enabling Anomali to automatically pull the logs from S3 whenever it receives a new notification from the queue.

Onboarding Steps

Step 1: Ship data to S3 using NXLog

See Using NXLog to Ship Data to set up NXLog to send data into S3.

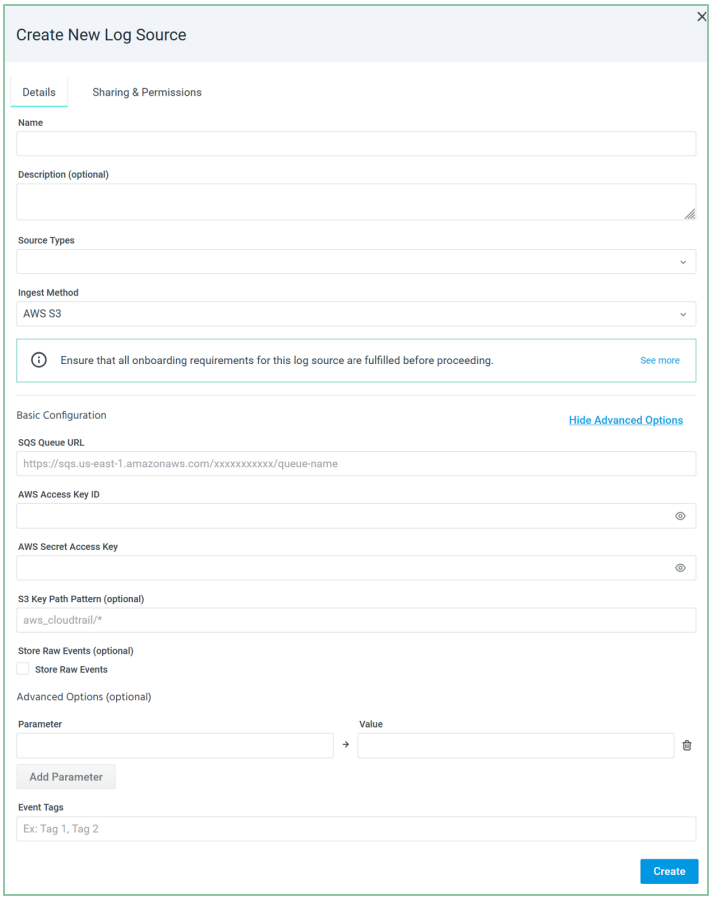
Step 2: Set up SQS queue

Once your data is in S3, you can send it to Anomali using Amazon SQS. See Setting up Amazon SQS queue for more information.

Step 3: Enable AWS S3 notifications

Enable AWS S3 notifications for Amazon SQS to receive change notifications when you add logs. See Amazon's guide to configuring AWS S3 notification for SQS for more information.

Step 4: Add Zscaler LSS Auth as new log source



On the Anomali platform, add Zscaler LSS Auth as a new log source, as follows:

1. Navigate to **Search** > **Log Source Management**.
2. Click **New** to add a new log source.
3. Enter a name for the log source.
4. (Optional) Enter a description for the log source.
5. Select it as the log source.
6. Select AWS S3 as the ingest method.
7. Ensure S3 notification are enabled. See "Step 2: Enable AWS S3 notifications" on page 442 for more information.
8. Provide the Basic Configuration details:

a. **AWS SQS Queue URL**: Enter the URL of your AWS SQS queue. See Setting up Amazon SQS queue for more information.

b. **AWS Secret Access Key**: Provide the AWS secret access key.

c. **AWS Access Key ID**: Enter the AWS Access ID.

d. **File Selector**: Provide the path to the event log data files. Anomali recommends the following practices for the path:

- Sourcetype must be the path prefix, as follows: `<sourcetype>/year=2025/month=04/day=05/path/to/file`. For example: `zscaler_lss_auth/year=2025/month=03/day=22/events/event_data_logs/`.
- Sourcetype name must not contain any spaces: For example, `"zscaler_lss_auth"` is correct, however `"Zscaler LSS Auth"` is incorrect.

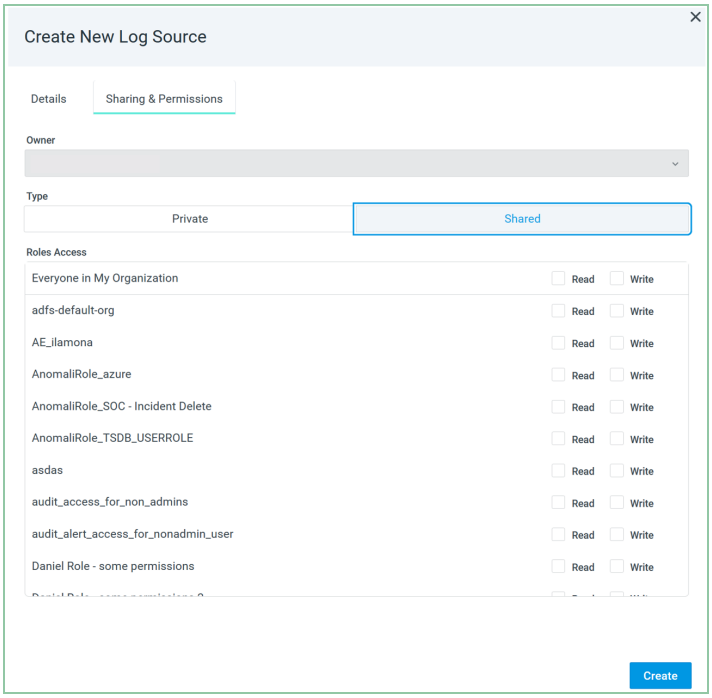
9. (Optional) Next to the Basic Configuration section, click on the **Advanced Options** link to provide additional information about the event log data:

   a. Enter one or more parameters that provide additional context about the data. For example, "File format" indicates the format of the event log data being shipped, or "File extension" that indicates the extension of the logs.

   b. Enter the corresponding value of the parameter. For example, CSV is a file format. Similarly, ".gzip" is a file extension.

10. Click **Save** to add the log source.

Step 5: Configure permissions



You can set permissions to decide which roles can view, add, or edit log sources. To do so, configure the following parameters:

1. Owner: Select an owner of the view from the list of users. This is the email address of the owner.
2. Type: Select the type of permission assigned to the view:
   a. Private: Only the owner has read and write privileges, that is, no other user can access or edit the view.
   b. Shared: Allows you to set the read-write privileges for a role that is mapped to different users, granting read-write permissions to all users assigned that role. You can also assign read or write permissions to everyone in your organization.

Step 6: Check log source status

Once added, the status of the log source becomes `Create Requested`. See Log Source Statuses to understand the different types statuses assigned to log sources.

Step 7: Receive confirmation email

You will receive a notification email from Anomali once you have created a new log source request. The Log Source Management page will show the status as `Create Requested`.

Once the log source has been provisioned and is ready for use, Anomali will send you another email and the Log Source Management page status for the log source will change to `Active`.

Log Transport Services (Limited Availability)

Anomali supports the following log transport services to ship the data from the customer's environment to Anomali Security Analytics.

- Amazon Simple Queue Service (SQS)

Setting up SQS Queue (Limited Availability)

This article helps you configure Amazon Simple Queue Service (SQS) as a log transport to ship event logs.

Step 1: Set up an SQS queue

Anomali recommends that you create a **standard** SQS queue. You can create a standard queue by following Amazon's guide to creating a standard queue.

Step 2: Create an IAM user

Once you successfully set up your queue, you must create an IAM user. See Amazon's guide to Create an IAM user for more information.

Step 3: Grant necessary permissions

While creating an IAM user, you must ensure your IAM user policy grants Anomali all the necessary permissions to pull and read data, depending on any change notifications the queue receives.

In the example code block below, the IAM user policy grants Anomali the following permissions:

1. **Decryption**: If your S3 bucket data is encrypted by Amazon Key Management System (KMS), Anomali must decrypts the logs. In the example below, the data is encrypted by the KMS key `ebf456c-39fa-67ff-bae1-95710483d2f7`. KMS key UUIDs are alphanumeric IDs that contain `0-9` and `a-f`.

   > **Note**: You must know the key used to encrypt your bucket that stores the logs. Contact your S3 account admin for more information.

2. **Queue actions**: Anomali gets the queue URL and attributes (such as ARN), receives and deletes messages, and can change the visibility timeout of a message.

3. **S3 user**: Anomali reads the logs from your S3 bucket, in this case named `anomali-cloudtrail-test`.

```
{
        "Version": "2012-10-17",
        "Statement": [
                {
```

```
                        "Sid": "KMS",
                        "Effect": "Allow",
                        "Action": [
                                "kms:Decrypt",
                                "kms:GenerateDataKey"
                        ],
                        "Resource": [
                                "arn:aws:kms:us-east-1:123456789012:key/0b29456c-39fa-67ff-bae1-95710483d2
                        ]
                },
                {
                        "Sid": "SQS",
                        "Effect": "Allow",
                        "Action": [
                                "sqs:DeleteMessage",
                                "sqs:GetQueueUrl",
                                "sqs:ChangeMessageVisibility",
                                "sqs:ReceiveMessage",
                                "sqs:GetQueueAttributes"
                        ],
                        "Resource": [
                                "arn:aws:sqs:us-east-2:123456789012:queue2"
                        ]
                },
                {
                        "Sid": "S3",
                        "Effect": "Allow",
                        "Action": [
                                "s3:GetObject"
                        ],
                        "Resource": [
                                "arn:aws:s3:::anomali-cloudtrail-test/*"
                        ]
                }
        ]
}
```

See Amazon's guide to create a custom Amazon SQS access policy and how SQS works with IAM for more information on IAM policies.

Step 4: Retrieve access keys

While creating the IAM user for Anomali, securely note your Access Key ID and Secret Access Key. These credentials are required to create a new log source in the Anomali platform.

If you don't have your Access Key ID and Secret Access Key set up, see Amazon's guide to Create New Access Keys for an IAM User.

Step 5: Obtain SQS queue URL

To create a new log source in the Anomali platform, you will also need the queue URL. To obtain the URL:

1. Sign in to your AWS Management console.
2. Navigate to the AWS SQS dashboard.
3. Click on the name of the queue you created to send logs to Anomali.

The queue URL is displayed in the **Details** section.

Using NXLog to Ship Data

Anomali Security Analytics can ingest event log data from NXLog when it is routed through AWS Simple Storage Service (S3). Anomali provides the S3 bucket. Your organization must configure NXLog to send logs to it. Multiple network devices from your organization can feed into a single S3 bucket.

Before You Begin

- Your organization must have a dedicated AWS S3 bucket provided by Anomali. Contact Anomali Customer Support to request an S3 bucket. Anomali will provide you access key and secret key once your S3 bucket is set up.
- Your organization must have an enterprise license for NXLog. Contact Anomali Customer Support to request the license.
- Your organization must have virtual machines (VMs). The number of VMs depends on the volume of logs you need to ingest. If you have huge log volumes, Anomali recommends the following minimal requirements for each VM:
  - Linux-based OS
  - 4 core CPU
  - 8–16 GB of RAM

Step 1. Set Up NXLog Enterprise Edition Agent

Install an NXLog Enterprise Edition agent. For more information on how to install an NXLog Enterprise Edition agent, see https://docs.nxlog.co/refman/current/index.html.

Step 2. Deploy NXLog Agent

Deploy the NXLog agent. For more information on how to deploy the NXLog agent, see https://docs.nxlog.co/userguide/deploy/index.html.

Step 3. Prepare Configuration File

1. Create a configuration file based on your requirements and the OS that you use. For more information of the configuration file structure, see

https://docs.nxlog.co/userguide/configure/overview.html.

2. In the Input section of your configuration file, specify the information about the input modules for sources of your logs:

```
<Input udp>
        Module        im_udp
        ListenAddr    IP::port
        BatchSize     3000
        BatchFlushInterval 300
</Input>
```

3. In the Output section of your configuration file, specify the information about log destination, which is the S3 bucket provided by Anomali:

```
<Output s3>
        Module       om_amazons3
        Region       us-east-1
        Bucket       bucket name
        Server       name of technology
        AccessKey    your Anomali-provided access key
        SecretKey    your Anomali-provided secret key
</Output>
```

For more information on AWS S3 configuration, see https://docs.nxlog.co/refman/current/om/amazons3.html.

4. In the Route section of your configuration file, specify the name of your input module and S3 output in the path:

```
<Route udp_aws_s3>
        Path          udp => s3
</Route>
```

5. Verify whether your configuration is correct. For this, see https://docs.nxlog.co/refman/current/man-nxlog.html.

> **Note:** In case of any issues, contact Anomali Customer Support to set up log ingestion for your organization.

Reference Information

This section contains additional information on different aspects of Anomali Security Analytics.

Refer to the following topics for more information:

Appendix A: Reserved Field Names and Keywords

The Anomali Security Analytics log parser leverages Logstash. Logstash is an open-source server-side data processing pipeline that is a component of many widely used data management systems. The following tables provides a list of Logstash keywords that you should avoid when you are adding field names, or you are specifying a pattern in the field for a custom log source.

Reserved Name	Usage
dsname dstype	These field names are reserved and used internally by Logstash.
host	The field name `host` is a reserved field name used by Logstash. Instead, use `host1` or something similar.
internal_dstype internal_dsname	These field names are reserved and used internally by Logstash.
message	The field name `message` is the field name used by Logstash to hold the original log message. Using this name as a new field overwrites the original message (Sample Line) contained in the field.
raw_event	This field name is reserved and used internally by Logstash.
tags	This field name is reserved and used internally by Logstash.
@timestamp timestamp1	These field names are reserved and used internally by Logstash.
@version	This field name is reserved and used internally by Logstash.

Appendix B: Sample Patterns for Dissect, Grok, Regex, and Ruby Parsers

Custom log sources can implement user-defined parsers. Anomali provides sample patterns for programmable sub parsers.

> **Caution:** Copying and pasting the samples from this PDF directly into the Anomali Security Analytics UI can sometimes result in syntax errors. If you get such errors, manually make the corrections in the UI.

Dissect

Dissect is a Logstash filter used to extract fields from log data. The following table provides examples of patterns commonly used to parse event logs.

Dissect Pattern	Example
%{clientip}	1.2.3.4
%{status}	200
%{request}	/english/venues/cities/images/montpellier/18.gif
%{size}	3171
%{httpversion}	1.1
%{method}	GET
%{url}	http://www.google.com/bot.html
%{@timestamp}	30/Apr/1998:22:00:52 +0000

Grok

Grok is a Logstash filter used to extract fields from log data. The following table provides examples of patterns commonly used to parse event logs.

Grok Pattern	Example
%{URIPATH:uri_path}	/v2/blacklist/
%{NUMBER:response_status}	15824, 0.043
%{WORD:method}	GET,production
%{GREEDYDATA:body}	any sentence
%{INT:port}	1234
%{IPORHOST:ip}	55.3.244.1
%{URI:url}	http://sylvaclouds.eu/new1/IMG-0001-documents.exe
%{DATESTAMP:datetime}	2017-09-27 0:21:12
%{SYSLOGTIMESTAMP:date}	Jun 2 14:55:46

Regex

Regex is short for regular expression. A regular expression specifies a string search pattern. The following table provides examples of regex patterns commonly used to extract fields from unstructured data.

Regex Pattern	Example
(?<ip>([0-9]{1,3}.){3}[0-9]{1,3})	38.99.50.98
(?<port>\d+)	8554
(?<method>\w+)	GET
(?<action>\w+\s\w+).	session miss.^M
(?<url>(?:https?:)(?:/[A-Za-z0-9$.+!*'(){},~:;=@#%_-]*)+)	http://sylvaclouds.eu/new1/IMG-0001-documents.exe
(?<hostname>[\w-]+)	elb-shop-com

Regex Pattern	Example
(?<status>\d{1,3})	200
(?<customer_uri>[^/]+$)	customerURI=/All Customers/ANSI/ANSI/740663
(?<uri_path>(?:/[A-Za-z0-9$.+!*'(){},~:;=@#%_-]*)+)	/Users/jdoe/Downloads/110
(?<hash>(^[a-fA-F0-9]{32}$)\|(^[a-fA-F0-9]{40}$)|(^[a-fA-F0-9]{64}$))	Matches md5 or sha1 or sha256
(?<event_time>([\d{2,4}-]+){2}\d{2}\s([\d:]+){2}\d{2})	2017-09-25 23:27:36
(?<timestamp>[\d-]+\w[\d:.-]+)	2019-10-20T23:00:26.059475-07:00
\<\d+\>(?<datetime>\d{2,4}[-/\s][A-Za-z]{3,9}[-/\s]\d+\s[\d:]+)	<14>2019 Jun 22 16:24:05
(?<datetime>[A-Za-z]{3,9}\s[A-Za-z]{3,9}\s[0-9]{1,2}\s[\d:]+)	Fri Aug 5 22:11:53 2011

Ruby

Ruby is a programming language that can be used to extract fields from unstructured data. The following table provides examples of Ruby logic commonly used to parse unstructured data.

Ruby Pattern	Example
def filter(event) date = event.get("date") time = event.get("time") if (not date.nil?) and (not time.nil?) date_time = "#{date}T#{time}" event.set("date_time", date_time) end return [event] end	Merges two fields: date=2018-07-10 time=22:31:14

Ruby Pattern	Example
def filter(event) if event.get('srcip') == 'localhost' return [] end return [event] end	Drops events that matches srcip=localhost.
def filter(event) date = event.get("<189>date") date = date.sub!("2018", "2021") event.set("date", date) return [event] end	Replaces date from 2018 to 2021.
def filter(event) service = event.get("service") _1, _2 = service.split(":") event.set("service_port", _2) return [event] end	Splits line using delimiter (eg - service=udp/port:7001).
def filter(event) url = event.get("cs_Referer") if (not url.nil?) and url.start_with? ("https://urlscan.io") tags = Array(event.get("tags")) # note that Array(nil) => [] tags << "drop_this_event" event.set("tags", tags) end return [event] end	Drops events that match cs_referer=https://urlscan.io using tags.

Ruby Pattern	Example
def filter(event) events = [] ["1st event", "2nd event", "3rd event"].each do |name| e = event.clone e.set('event_name', name) events << e end return events end	Splits a single event into three events.

Appendix C: ThreatStream Indicator Types

This appendix lists the indicator types (iTypes) available to Anomali Security Analytics from Anomali ThreatStream.

> **Note:** In ThreatStream, indicators have value types Domain, Email, Hash, IP, URL, and String. Security Analytics does not support correlation with indicators having String value types.

Indicator Type	Name	Type	Severity	Description
actor_ip	Actor IP	IP	Low	IP address associated with a system involved in malicious activity. Example: itype="actor_ip"
adware_domain	Adware Domain	Domain	Low	Domain name associated with adware or other Potentially Unwanted Applications (PUA). Example: itype="adware_domain"
anon_proxy	Anonymous Proxy IP	IP	Low	IP address of the system on which anonymous proxy software is hosted. Example: itype="anon_proxy"
anon_vpn	Anonymous VPN IP	IP	Low	IP address associated with commercial or free Virtual Private Networks (VPN). Example: itype="anon_vpn"

Indicator Type	Name	Type	Severity	Description
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"
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_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"

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"
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_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"
bot_url	Infected Bot URL	URL	Low	URL of an infected machine acting as an autonomous bot. Example: itype="bot_url"
brute_ip	Brute Force IP	IP	Low	IP address associated with password brute force activity. Example: itype="brute_ip"

Indicator Type	Name	Type	Severity	Description
c2_domain	Malware C&C Domain Name	Domain	High	Domain name used by malware for command and control communication. Example: itype="c2_domain"
c2_ip	Malware C&C IP Address	IP	High	IP address used by malware for command and control communication. Example: itype="c2_ip"
c2_url	Malware C&C URL	URL	High	URL used by malware for command and control communication. Example: itype="c2_url"
comm_proxy_domain	Commercial Webproxy Domain	Domain	Low	Domain of the system on which commercial proxy software is hosted. Example: itype="comm_proxy_domain"
compromised_domain	Compromised Domain	Domain	Low	Domain name of website or server that has been compromised. Example: itype="compromised_domain"
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"

Indicator Type	Name	Type	Severity	Description
compromised_ip	Compromised IP	IP	Low	IP address of website or server that has been compromised. Example: itype="compromised_ip"
compromised_url	Compromised URL	URL	Medium	URL of the website or server that has been compromised. Example: itype="compromised_url"
crypto_hash	Cryptocurrency Mining Software	Hash	High	File hash for cryptocurrency mining software. Example: itype="crypto_hash"
crypto_ip	Cryptocurrency IP	IP	High	IP address associated with a cryptocurrency mining software. Example: itype="crypto_ip"
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"
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
disposable_email_domain	Disposable Email Domain	Domain	Low	Domain associated with disposable email activity. Example: itype="disposable_email_domain"
downloader_domain	Downloader Domain	Domain		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"
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"

Indicator Type	Name	Type	Severity	Description
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"
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_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_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 fraudulent activity. Example: itype="fraud_domain"
fraud_email	Fraud Email	Email	Low	Email address associated with fraudulent activity. Example: itype="fraud_email"
fraud_ip	Fraud IP Address	IP	High	IP address associated with fraudulent activity. Example: itype="fraud_ip"
fraud_md5	Fraud Hash	Hash	Very High	Hash associated with fraudulent activity. Example: itype="fraud_md5"

Indicator Type	Name	Type	Severity	Description
fraud_url	Fraud URL	URL	Medium	URL associated with fraudulent activity. Example: itype="fraud_url"
free_email_domain	Free Email Domain	Domain	Low	Domain associated with free email service activity. Example: itype="free_email_domain"
geolocation_url	IP Geolocation URL	URL	Low	URL that can be used to provide IP Geo location services. Example: itype="geolocation_url"
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"
i2p_ip	I2P IP Address	IP	Low	IP address observed to be connecting to the I2P (Invisible Internet Project) network. Example: itype="i2p_ip"
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"

Indicator Type	Name	Type	Severity	Description
infostealer_ip	Information Stealer IP	IP	Very High	IP address associated with an information stealer. Example: itype="infostealer_ip"
infostealer_ url	Information Stealer URL	URL	Very High	URL associated with an information stealer. Example: itype="infostealer_url"
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_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"
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_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_md5	Malware File Hash	Hash	Very High	MD5 or SHA hash of malware sample. Example: itype="mal_md5"

Indicator Type	Name	Type	Severity	Description
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_url	Malware URL	URL	Very High	URL contacted by malware sample when run on an infected host. Example: itype="mal_url"
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"
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"
parked_url	Parked URL	URL	Low	URL of a website that is currently parked. Example: itype="parked_url"

Indicator Type	Name	Type	Severity	Description
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"
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_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"

Indicator Type	Name	Type	Severity	Description
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"
pos_domain	Point of Sale Malicious Domain	Domain	Medium	Domain associated with malware targeting Point of Sales systems. Example: itype="pos_domain"
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_url	Point of Sale Malicious URL	URL	Medium	URL associated with malware targeting Point of Sales systems. Example: itype="pos_url"

Indicator Type	Name	Type	Severity	Description
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"
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_url	Ransomware URL	URL	Very High	URL associated with ransomware. Example: itype="ransomware_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"

Indicator Type	Name	Type	Severity	Description
scan_ip	Scanning IP	IP	Medium	IP address observed to perform port scanning and vulnerability scanning activities. Example: itype="scan_ip"
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"
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"
spam_ domain	Spam Domain	Domain	Low	Malicious domain name contained in the SPAM email messages. Example: itype="spam_ domain"

Indicator Type	Name	Type	Severity	Description
spam_email	Spammer Email Address	Email	Low	Email address that has been observed sending SPAM emails. Example: itype="spam_email"
spam_ip	Spammer IP	IP	Low	IP address that is known to send SPAM emails. Example: itype="spam_ip"
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"
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"

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_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_ 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"

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"
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"
torrent_ tracker_url	Torrent Tracker URL	URL	Low	URL used for tracking bittorrent file transfer activity. Example: itype="torrent_ tracker_url"
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"

Indicator Type	Name	Type	Severity	Description
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_url	Trojan URL	URL	High	URL associated with a Trojan malware that disguises as a legitimate code or software. Example: itype="trojan_url"
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"
vuln_risk_score	Vulnerability Risk Score	String	Low	Risk score for a vulnerability. Example: itype="vuln_risk_score"
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"

Indicator Type	Name	Type	Severity	Description
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"

Appendix D: Anomali Security Analytics Alert Messages

This appendix provides a reference of Security Analytics alert message fields.

Alert messages can be forwarded to Splunk HTTP Event Collector (recommended) or to a secure syslog server (TCP only).

The information is provided to help you parse alert messages received from Security Analytics.

Alert Message Format

Security Analytics can send the messages in the following formats:

- JSON (recommended)

  The alert message contains the fields listed in the reference table below. Fields that were not populated during correlation have empty values.

- CEF

  Security Analytics fields are modified to conform with the CEF format described in the ArcSight Common Event Format reference. The alert message contains the fields listed in the reference table below. Fields that were not populated during correlation have empty values.

JSON

The following is an example of an IOC alert message in JSON format:


```
{"age": "46", "app_type": "universal_link", "asn": "",
"attackpattern_ids": "[2419]", "cim_field": "ulink_
summary:src|src_ip|dest|dest_ip|url|http_referrer|file_hash|file_
hash2|file_hash3|sender|receiver", "classification": "private",
"confidence": "70", "corr_type": "iocmatch", "count": "1",
"country": "", "date_first": "2022-12-19T13:49:46.110429", "date_
last": "2022-12-19T13:49:46.110429", "dcid": "604", "detail":
"kill-chain:-actions-on-objectives-(lockheed-martin-cyber-kill-
chain),kill-chain:-command-and-control-(lockheed-martin-cyber-
kill-chain),kill-chain:-command-and-control-(mitre-attack),kill-
chain:-execution-(mitre-attack),kill-chain:-impact-(mitre-
attack),kill-chain:-installation-(lockheed-martin-cyber-kill-
chain),source:www.microsoft.com", "detail2": "imported by user 1",
"domain": "", "event_time": "2023-02-03T22:30:00Z", "id":
"17667902", "import_session_id": "", "indicator":
```

"b301c4b060dadf887e53d671aa6a7aff", "indicator_type": "md5", "ioc_match_id": "1_4221577028_6_17667902", "itype": "mal_md5", "lat": "", "loc": "", "lon": "", "match_count": "1", "match_distinctive_count": "1", "match_records_time_window": ["2023-02-03T22:30:00Z", "2023-02-03T22:30:00Z"], "md5": "b301c4b060dadf887e53d671aa6a7aff", "org": "", "originator": "1", "resource_uri": "/api/v1/intelligence/17667902", "severity": "medium", "source_feed_id": "887", "span": "10m", "src_host": "X.X.21.76", "srcip": "", "state": "active", "timestamp": "1675463729680", "tm_ids": "2419", "tm_names": "Scheduled Task/Job: Scheduled Task", "tm_type": "attackpattern", "trusted_circle_ids": "", "volume": "90989568", "tags": "", "alert_time": "2023-02-04T00:40:19.687484Z", "rule_type": "simple", "match_type": "attackpattern", "source_feed": "SEKOIA.IO Threat Intelligence QA", "event.process_id": 0, "event.file_hash": "b301c4b060dadf887e53d671aa6a7aff", "event.sourcetype": "Cisco:ASA", "event.src_ip": "X.X.21.76", "event.bytes_in": 0, "event.dest_port": 0, "event.action": "allow", "event.host": "qatest1", "event.user": "294682@qq.com", "event.dest_ip": "X.X.21.242", "event.dest": "nayablabs.com", "event.url": "http://milinkes.myhostpoint.ch/ING/ingdirect.es/9cdc7/pass.html", "event.src_port": 0, "event.sender": "294682@qq.com", "event.src": "X.X.21.76", "event.bytes_out": 0, "alert_batch_id": "6697349", "alert_rule_name": "HEC_http_attackpattern"}

CEF

The following is an example of an alert in CEF format:

CEF:0|Anomali|Anomali Enterprise|5.0.0|apt_domain|cef_HEC_vul_https_Continuous|very-high|actorIds=[3931] age=1057 appType=universal_link cn2= cn2Label=asn campaignIds=[9821] cimField=ulink_summary:src|src_ip|dest|dest_ip|url|http_referrer|file_hash|file_hash2|file_hash3|sender|receiver classification=private clientId= cn1=83 cn1Label=confidence corrType=iocmatch cnt=1 cs5= cs5Label=country dateFirst=1584123864886 dateLast=1675218036698 dcid=604 cs4=xdresponse:dns cs4Label=tags detail2=imported by user 1 domain=1iba3khx0etvrmccz7may3eh8v.net email= end=1675463400000 id=4597048 importSessionId=560.0 cs2=1iba3khx0etvrmccz7may3eh8v.net cs2Label=domain iocMatchId=1_4221577016_1_4597048 lat= loc= lon= matchCount=1 matchDistinctiveCount=1 matchRecordsTimeWindow=2023-02-03T22:30:00Z,2023-02-03T22:30:00Z org= deviceDirection=1

```
cs6=/api/v1/intelligence/4597048 cs6Label=resource_uri
sourceFeedId=0 span=10m srcHost=X.X.115.72 srcip= state=active
timestamp=1675463729680 tipreportIds=[7243, 7244, 7245, 7240,
7241] flexString2=639 flexString1=Wikimedia MediaWiki 1.31
CentralAuth Unspecified Vulnerability
flexString1Label=vulnerability ttpIds=[1502] url= volume=90983424
vulnerabilityIds=[634, 636, 638, 647, 654, 659, 660, 672, 677,
680, 656, 661, 663, 665, 669, 670, 674, 679, 685, 688, 690, 662,
668, 671, 675, 682, 695, 698, 628, 630, 631, 641, 644, 649, 658,
667, 678, 687, 691, 697, 629, 632, 633, 635, 640, 645, 646, 648,
650, 651, 652, 657, 666, 673, 676, 681, 683, 684, 689, 693, 694,
637, 639, 642, 643, 653, 655, 664, 686, 692, 696] tags=
alertTime=1675471320855 ruleType=simple matchType=vulnerability
cs3=tech@threatstream.com cs3Label=source_feed eventProcessId=0
fileHash=e6a9d9791f763123f9fe1f69e69069340e02248b9b16a88334b6a5a61
1944ef9 cs1=Cisco:ASA cs1Label=sourcetype src=X.X.115.72
eventBytesIn=0 dpt=0 act=allow eventHost=qatest1
suser=294682@qq.com dst=X.X.214.206
dhost=1iba3khx0etvrmccz7may3eh8v.net
request=http://X.X.4.132/i.htm spt=0 shost=X.X.115.72
eventBytesOut=0 cn3=6697637 cn3Label=alert_batch_id
```

Alert Message Fields

The following table describes alert message fields. The first seven fields listed are standard CEF fields. These fields are always the first seven fields in a CEF message, and these fields are not listed as name=value pairs (only values are expected). IOC alert messages have the same event-related fields but different intelligence-related fields.

JSON Field	CEF Field	Value	Description
	<cef_version>	string	Example: CEF:0
	<vendor>	string	Example: Anomali
	<product>	string	Example: Anomali Enterprise
	<version>	string	Example: 5.0.0
	<event class ID>	string	apt_domain

JSON Field	CEF Field	Value	Description
	<name>	string	The CEF <name> field is mapped from Security Analytics field alert_rule_name. Example: cef_HEC_vul_https_Continuous This field appears only when the alert configuration option **Output Raw Only** is not selected. If the option is selected, this standard CEF field contains the value `unknown`.
	<severity>	string	The CEF <severity> field is mapped from the Security Analytics field severity. Example: very-high
_raw_id		numeric	Internal.
actor_ids	actorIds	numeric	Associated actor IDs in ThreatStream. Example: [2342, 2313]
age	age	numeric	Event time - intel first seen. Example: 34
alert_batch_id	cn3= cn3Label=alert_batch_id	string	This field appears only when the alert configuration option **Output Raw Only** is not selected. Internal.
alert_rule_name	See <name> above.	string	This field appears only when the alert configuration option **Output Raw Only** is not selected. Alert configuration name.

JSON Field	CEF Field	Value	Description
alert_time	alertTime	date	This field appears only when the alert configuration option **Output Raw Only** is not selected. Timestamp when the alert was triggered. **Notes:** • In the results table, the time displayed is UTC time, adjusted for the browser time zone. • When you form search expressions, specify UTC time in the following format: <YYYY><MM><DD>T<HH>:<MM>:<SS>. The date part and the time part are separated by a capital T. You do not need to include T and the time values if you intend to search by date only. The following is an example of UTC time format: `2022-01-05T00:00:00` • You can also specify a time zone offset for searches where time zone precision is important. In the following example, the time zone offset is the `-08:00` at the end: `2022-01-05T00:00:00-08:00` • In exported results, the date and time are displayed as epoch time values. The following example shows the previous date-time example in epoch format: `1641342478`

JSON Field	CEF Field	Value	Description
app_type	appType	string	Link type. Example: splunk, universal_link
asn	cn2 cn2Label=asn	string	Autonomous system number. Example: 48780
asset_dest_criticality		string	Criticality assigned an asset. Example: low, medium, high, critical
asset_dest_dept		string	Department of an asset. Example: engineering, hr, finance
asset_dest_hostname		string	Hostname or FQDN of an asset. Example: qa_jenkins.example.com
asset_dest_ip		string	IP address of an asset. Example: 192.168.10.77
asset_dest_location		string	Location of an asset. Example: Redwood City headquarters
asset_dest_vulnerability		string	Vulnerabilities reported by the asset scanner. Example: CVE-2022-31214
asset_src_criticality		string	Criticality assigned an asset. Example: low, medium, high, critical
asset_src_dept		string	Department of an asset. Example: engineering, hr, finance
asset_src_fqdns		string	Fully-qualified domain name. Tenable.io scanner reports include a FQDN field for assets. Example: example.com

JSON Field	CEF Field	Value	Description
asset_src_hostname		string	Hostname or FQDN of an asset. Example: qa_jenkins.example.com
asset_src_ip		string	IP address of an asset. Example: 192.168.10.77
asset_src_location		string	Location of an asset. Example: Redwood City headquarters
asset_src_vulnerability	flexString1 flexString1Label=vulnerability	string	Vulnerabilities reported by the asset scanner. Example: CVE-2022-31214
attackpattern_ids		numeric	Associated attack pattern IDs in ThreatStream. Example: [2342, 2313]
campaign_ids	campaignIds	numeric	Associated campaign IDs in ThreatStream. Example: [2342, 2313]
cim_field	cimField	string	Fields to correlate with the global threat intelligence. Example: ulink_summary:src|src_ip|dest|dest_ip|url|http_referrer|file_hash|file_hash2|file_hash3|sender|receiver|query
classification	classification	string	Classification as public or private intelligence. Example: public or private
client_id	clientID	numeric	Reserved for MSSP. 0 in non-MSSP deployment. The combination of customer_id and customer_name defines its value. Example: 1

JSON Field	CEF Field	Value	Description
confidence	cn1 cn1Label=confidence	numeric	Confidence score assigned to the indicator. Example: 85
corr_type	corrType	string	Correlation type set by correlation_engine. Example: iocmatch, dgamatch
count	cnt	numeric	Aggregate event count. Example: 1
country	cn5 cn5Label=country	string	Country associated with the indicator. Example: US
date_first	dateFirst	date	First seen on ThreatStream. Example: 41914.8642939815
date_last	dateLast	date	Last updated on ThreatStream. Example: 41914.8642939815
dcid	dcid	string	Unique ID of a registered link. Example: 67857e18-6ce5-480d-a72a-6ec12102a4bf
detail	cs4 cs4Label=tags	string	Additional comments and context. Example: popularity=low, malware
detail2	detail2	string	Deprecated (v1).
dga_prob		numeric	DGA probability of a domain. Example: .98
do_realert		boolean	Internal. Link alert setting indicating whether to send an alert when the link or log source resumes receiving logs after a period of downtime.

JSON Field	CEF Field	Value	Description
domain	domain cs2= cs2Label=domain	string	Domain indicator value (v1). Example: www.example.com
ds_id		string	Unique ID of a data source of a registered link. Example: 5
email	email	string	Email indicator value (v1). Example: johndoe@amec.com
event.action	act	string	The action captured by the event. Example: allowed, blocked
event.answer		string	Answers for the DNS query. Example: ["10.10.10.10","10.10.10.11"]
event.app		string	The application detected. Example: Slack, Google Gmail, LinkedIn
event.bytes_in	eventBytesIn	numeric	How many bytes received by a network interface. Example: 347
event.bytes_out	eventBytesOut	numeric	How many bytes transmitted by a network interface. Example: 665
event.category		string	The category of alert (azure security alert). Example: credentialTheft, ransomware

JSON Field	CEF Field	Value	Description
event.command_line		string	The full command string of the spawned process. Example: `"\"procdump.exe\" -mals"`
event.dest	dhost	string	The destination of network traffic. Example: 52.233.72.222 or www.google.com Note: Correlated with indicators of type ip or domain.
event.dest_ip	dst	string	The IP address of the destination. Example: 52.233.72.222 Note: Correlated with indicators of type ip.
event.dest_port	dpt	numeric	The destination port of network traffic. Example: 80, 443, 8080
event.ds_id		string	Unique id of a data source in a registered link. Optional. Example: 5
event.ds_type		string	Type of a data source in a registered link. Optional. Example: qradar, sumo. az_sentinel, syslog
event.event_id		string	A Windows identification number that specifies the event type. Example: 4624
event.event_name		string	The name of an event. Example: DnsRequest, ProcessRollup2

JSON Field	CEF Field	Value	Description
event.file_hash	fileHash	string	A cryptographic identifier assigned to the file object affected by the event. Example: e0d123e5f316bef78bfdf5a008837577 Note: Correlated with indicators of type md5.
event.file_hash2		string	A cryptographic identifier assigned to the file object affected by the event. Example: 56857cfc709d3996f057252c16ec4656f5292802 Note: Correlated with indicators of type md5.
event.file_hash3		string	A cryptographic identifier assigned to the file object affected by the event. Example: ba7816bf8f01cfea414140de5dae2223b00361a396177a9cb410ff61f20015a Note: Correlated with indicators of type md5.
event.file_name		string	The name of the file. Example: notepad.exe
event.file_path		string	The folder containing the file. Sigma name: FilePath Example: C:\Program Files (x86)\VMware\VMware Workstation
event.host	eventHost	string	VM host name or IP address that link is deployed on. Example: 198.51.100.0
event.http_method		string	The HTTP method used in the request. Example: get, post, delete, patch

JSON Field	CEF Field	Value	Description
event.http_referrer		string	The HTTP referrer used in the request. Example: https://example.com/ Note: Correlated with indicators of type url.
event.image		tring	The executable name of the process. Sigma name: Image, ProcessName, OriginalFileName, TargetImage, TargetFileName Example: svchost.exe
event.message_id		string	The globally-unique message identifier. Example: 123e4567-e89b-12d3-a456-426655440000
event.original_file_name		string	Original name of the file that was changed. Example: "test.pdf"
event.parent_command_line		string	The full command string of the parent process. Example: C:\Windows\System32\svchost.exe -k WerSvcGroup
event.parent_image		string	The executable name of the parent process. Example: notepad.exe
event.parent_process_id		string	The numeric identifier of the process assigned by the operating system. Example: 4834

JSON Field	CEF Field	Value	Description
event.platform		string	The operating system of the asset. Sigma name: Platform Example: win, mac, linux
event.process_id	eventProcessId	numeric	The numeric identifier of the process assigned by the operating system. Example: 3683
event.protocol		string	The network/email protocol. Example: http, tcp, udp, smtp
event.query		string	The domain that needs to be resolved in a DNS query. Example: www.google.com Note: Correlated with indicators of type domain.
event.receiver	email	string	The email address of the message recipient. Example: john.doe@amce.org Note: Correlated with indicators of type email.
event.record_type		string	The DNS resource record type. Example: A, CNAME, MX, NS, PTR, AAAA
event.reg_key		string	Registry key that the recorded action was applied to. Sigma name: TargetObject Example: HKEY_LOCAL_MACHINE\SOFTWARE\RegisteredApplications

JSON Field	CEF Field	Value	Description
event.reg_value_data		string	Data of the registry value that the recorded action was applied to. Example: Software\Microsoft\Windows\CurrentVersion\Applets\Wordpad
event.reg_value_name		string	Name of the registry value that the recorded action was applied to. Example: "Wordpad"
event.return_code		string	The http status code or dns response code. Example: 200, 404, 504, NOERROR, NXDOMAIN
event.sender	email	string	The email address of the message sender. Example: bar@amce.org Note: Correlated with indicators of type email.
event.sourcetype	cs1= cs1Label=sourcetype	string	The device vendor. Example: PAN Traffic, Cisco ASA, Zscaler
event.src	src	string	The source of network traffic. Example: 192.168.134.3 or internaltest.qa.amce.org Note: Correlated with indicators of type ip or domain.
event.src_ip	shost	string	The IP address of the source. Example: 192.168.34.3 Note: Correlated with indicators of type ip.
event.src_port	spt	numeric	The source port of network traffic. Example: 8080

JSON Field	CEF Field	Value	Description
event.status		string	The status of the service.
event.subject		string	The subject of the message.
event.title		string	Alert title (Azure security alert).
event.ttl		numeric	The time-to-live of the network packet.
event.url	request	string	The fully qualified URL of the requested HTTP resource. Example: https://www.example.com/cgi-bin/search.cgi?q=example%20search Note: Correlated with indicators of type url.
event.user	suser	string	The user that requested the traffic flow. Example: john.doe@amce.org
event.user_agent		string	The user agent used in the request. Example: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0) Gecko/20100101
event_meta_id		numeric	Internal.
event_time		date	Time when the event was recorded on the device, in UNIX timestamp milliseconds. Example: 1614815939000
id	id	string	ID of an indicator. Example: 34566
import_session_id	importSessionId	string	ID of import session in which the indicator was imported. Example: 234

JSON Field	CEF Field	Value	Description
indicator		string	Value of an indicator. Example: 123.160.146.123, 2cd3e0df721f0c05e3c385e55e449bf5
indicator_type		string	Indicator value type. Example: ip, domain, url, email or md5
ioc_match_id	iocMatchId	string	Unique id. Format: {orgid}_{event_id}_0_{ioc_id} Example: 1773_79618005142_0_59324653376
itype		string	Indicator type. See appendix for reference. Example: apt_ip
last_activetime		date	Time that events were last received from the link or log source being monitored. Example: 2023-02-24T13:44:01.097635Z
lat	lat	numeric	Latitude associated with the Geo location of the IP address. Example: 48.199997
link_id		numeric	ID of the link or log source being monitored. Example: 135
link_name		string	Configuration name of the link or log source being monitored. Example: ulink_029
link_type		string	Type of the link or log source being monitored. Example: ulink

JSON Field	CEF Field	Value	Description
loc	loc	numeric	Internal.
lon	lon	numeric	Longitude associated with the Geo location of the IP address. 16.3667
malware_family		string	A group of applications with similar attack techniques. Example: conficker
match_count	matchCount	Numeric	Number of events that matched to trigger the alert. For Include/Exclude List and Simple Match rules, match_count = 1. For Frequency Detection and Spike Detection rules, match_count = *As specified in the Rule Specifics*
match_distinctive_count	matchDistinctiveCount	Numeric	Internal.
match_records_time_window	matchRecordsTimeWindow	Date	The time window examined by the alert rule. `2021-11-29T07:22:14+00:00`
match_type	matchType	String	This field appears only when the alert configuration option **Output Raw Only** is not selected. Type of alert query filter that matched. Example: `actor`
md5		string	File hash value. Example: 2cd3e0df721f0c05e3c385e55e449bf5

JSON Field	CEF Field	Value	Description
org	org	string	Registered owner (organization) of the IP address associated with the indicator. Example: Foundation for Applied Privacy
originator	deviceDirection	numeric	Network directionality. Example: 0-inbound, 1-outbound
resource_uri	csLabel= cs6Label=resource_uri	string	URI for the indicator. Example: /api/v1/intelligence/58027831945/
rule_type	rule_type	string	This field appears only when the alert configuration option **Output Raw Only** is not selected. Type of alert rule. Example: `simple`
severity	See <severity> above.	string	Severity assigned to the indicator. Example: low, medium, high, very-high
source		string	The source of the indicator. Example: crowdstrike, recorded future
source_feed	cs3= cs3Label=source_feed	string	Name of the source feed of the indicator.
source_feed_id	sourceFeedId	numeric	The source feed ID of the indicator. Example: 345
span	span	string	The time interval specified for the run. Example: 10m
src_host	srcHost	string	Takes the first non-null value of asset_src_hostname, src and src_ip. Example: 198.51.100.0

JSON Field	CEF Field	Value	Description
srcip	srcip	string	IP address value of an indicator (v1). Example: 1.2.3.4
state	state	string	Status assigned to the indicator. Example: active, inactive, falsepos
tags	tags	string	Additional comments and context. Example: malware, vitim_geo=in
timestamp	timestamp	date	Time when the event was processed by correlation engine, in unix timestamp milliseconds. Example: 1643398553853
tipreport_ids	tipreportIds	numeric	Associated threat bulletin IDs in ThreatStream. Example: [5473, 34724]
tm_ids		numeric	Threat Model ID information from ThreatStream.
tm_names		string	Threat Model name information from ThreatStream.
tm_type		string	Threat Model type information from ThreatStream.
trusted_circle_ids		numeric	A list of trusted circle IDs in ThreatStream assigned to the indicator. Example: [1, 45]
ttp_ids	ttpIds	numeric	Associated TTP IDs in ThreatStream. Example: [5473, 34724]
url	url	string	URL value of an indicator (v1). Example: http://somedomain.com/
volume	volume	string	Internal.

JSON Field	CEF Field	Value	Description
vulnerability_ids		numeric	Associated vulnerability IDs in ThreatStream. Example: [5473, 34724]

Appendix E: Using the Anomali Security Analytics RESTful API

Anomali Security Analytics is accessible through a REST API. The API allows you to perform some routine operations, such as posting asset data to Security Analytics and getting search results.

> **Notes:**
>
> - Only the API endpoints described in this document are supported.
> - API requests are limited to 1 request per minute.

About the API

The API offers bi-directional interaction with Security Analytics.

Accessing the API

To access the API related to Security Analytics, use the following base URL:

```
https://api.threatstream.com/api/v1/xdr/<resource>/
```

where

<resource> is an API endpoint; for example, `asset` or `usearch`.

Authenticating to ThreatStream

Making requests through the API requires authenticating to ThreatStream using your username (the email address associated with your ThreatStream account) and your dedicated API Key. You can find your username and API Key on the My Profile tab within ThreatStream settings.

Specifying your username and API Key in the header of the request is the most secure method of authentication. Anomali recommends using this authentication method.

```
curl 'https://api.threatstream.com/api/xdr/get_
version/' -H 'Authorization: apikey <username>:<api_
key>'
```

Using Operators

The first API operator called after the resource must start with a question mark and subsequent operators must begin with an ampersand.

```
curl 'https://api.threatstream.com/api/v1/xdr/api/v1/dga_
score/?domains=domain1,domain2' -H 'Authorization: apikey
<username>:<api_key>'
```

Time Formats

The Security Analytics API supports the time formats described in the following table.

Format	Description	Examples
Absolute Format	Date time string in ISO format	`2020-05-01T13:45:30.000000 -04:00`
Epoch	Date time string in epoch format.	`1623159474141`
Relative Format 1	Time in UTC $NOW format: "`now[/<boundary>]`" where *boundary* is W|w: round to Monday 12 am of the week D|d: round to 12 am of the day H|h: round to the beginning of the hour M|m: round to the beginning of the minute	`Now/w` `now/M`

Format	Description	Examples
Relative Format 2	Time in UTC $NOW format: "+|- <NUM> <unit>[/<boundary>]" where NUM is a numeral *unit* defines one of the following: Y|y: year, # one year is 365 days m: month, # one month is 30 days W|w: weeks, D|d: day, H|h: hour, M: minute, S|s: second, U|u: microsecond *boundary* is W|w: round to Monday 12 am of the week D|d: round to 12 am of the day H|h: round to the beginning of the hour M|m: round to the beginning of the minute	-30d/d -1y/M

Prerequisites

- A user ID and API key is required to access ThreatStream through the APIs. If you do not have these credentials, contact your ThreatStream Org Admin to create an account.
- APIs return attributes in the JavaScript Object Notation (JSON) format; therefore, familiarity with JSON is recommended.

Using REST APIs to Upload Asset Information

The REST API supports uploading asset data files.

Example CSV File

Download template files from Security Analytics. When possible, use the template_ip_to_hostname.csv file for your asset model. For information about asset file types, see "Managing Asset CSV File Imports" on page 343.

The following example shows the format of the CSV list in template_ip_to_hostname.csv:

```
ip,hostname,department,location,criticality,os,vulnerabilities,sca
nner
```

The following example shows example values for template_ip_to_hostname.csv:

```
192.168.XX.XX,host.example.com,engineering,NYC,high,Linux-Ubuntu-
18, CVE-2018-10561|CVE-2020-0822,test_scanner
192.168.XX.0/24,sales servers,Sales,Washington
D.C.,critical,Linux-Ubuntu-18,CVE-2014-2483,test_scanner
```

Task Overview

There are two steps to uploading an asset file:

"Step 1: Generate a Signed URL for the File Posting" below

"Step 2: Upload the File " on the next page

Step 1: Generate a Signed URL for the File Posting

This first step is to generate a signed URL and related values. You use the values returned in this step for the command in Step 2.

Request

/api/v1/xdr/asset/post_asset_file

HTTP Method: POST

Attributes

Attribute	Description
event_time	Current time.
file_type	Asset CSV template file type.

Example curl Command

```
curl -X 'POST' 'https://api.threatstream.com/api/v1/xdr/asset/post_asset_file/ \
    -H 'Authorization: apikey <username>:<api_key>'  \
    -H 'accept: application/json' \
    -H 'Content-Type: application/json' \
    -d '{
         "event_time": "1623159474141",
```

```
        "file_type": "ip"
        }'
```

Responses

Response Code	Example
200 Success	`{ "url": "https://XXXXXX.s3.amazonaws.com/", "fields": { "policy": <policy>, "AWSAccessKeyId": <AWSAccessKeyId>, "key": <key>, "signature": <signature> } }`
400 Invalid Parameter	`Invalid parameter {}`
500 Error	`Exception when posting file to s3 - {}`

Step 2: Upload the File

This second step is to upload the file. You use the values returned in Step 1.

The following example posts a file test.csv that resides in the local directory.

Example curl Command

```
curl -v -F "key=<key>" \ -F "AWSAccessKeyId=<AWSAccessKeyId>" \ -F
"Policy=<Policy>" \ -F "Signature=<Signature>" \ -F
"file=@test.csv" \ <url>
```

Using REST APIs to Get DGA Score Information

The REST API supports looking up the DGA score for specified domains. For information about DGA, see "DGA Match Activity Searches" on page 94.

Request

/api/v1/xdr/dga_score

HTTP Method: GET

Attributes

Attribute	Description
domains	Comma-separated list of domains to look up.

Example curl Command

```
curl -X 'GET' 'https://api.threatstream.com/api/v1/xdr/dga_
score/?domains=domain1.net,domain2.net' -H 'Authorization: apikey
<username>:<api_key>' -H 'accept: application/json'
```

Responses

Response Code	Example

200 Success	`{"data": {`
	`  "domain1.net": {`
	`  "registered_domain": false,`
	`  "probability": 1.0,`
	`  "malware_family": "Conficker,`
	`[...],Pykspa,Pykspa2,QakBot,Redyms,Tempedreve,Urlzone,Vidro"`
	`  },`
	`  "domain2.net": {`
	`  "registered_domain": false,`
	`  "probability": 1.0,`
	`  "malware_family": "Locky,Necurs,Nymaim,Recurs"`
	`  }`
	`  }`
	`}`

500 Error	`DGA score retrieval failed: {}`

Using REST APIs to Upload a DGA Exclude List

The REST API supports uploading a DGA exclude list file.

Example Exclude List File

The file must be a plain text file that specifies one domain per line. For example:

```
example.com
mytestdomain.com
xample.com
```

For information about exclude lists, see "Managing Exclude Lists" on page 273.

Task Overview

There are two steps to uploading an asset file:

"Step 1: Generate a Signed URL for the File Posting" below

"Step 2: Upload the File " below

Step 1: Generate a Signed URL for the File Posting

This first step is to generate a signed URL and related values. You use the values returned in this step for the command in Step 2.

Request

/api/v1/xdr/excludelist/dga/file/

HTTP Method: POST

Example curl Command

```
curl -X 'POST'
'https://api.threatstream.com/api/v1/xdr/excludelist/dga/file/' -H
'Authorization: apikey <username>:<api_key>' -H 'accept:
application/json'
```

Responses

Response Code	Example
200 Success	`{ "url": "https://XXXXX.s3.amazonaws.com/", "fields": { "policy": "<Policy>", "AWSAccessKeyId": "<AWSAccessKeyId>", "key": "<Key>", "signature": "<Signature>" } }`
500 Error	`Exception when posting file to s3 - {}.`

Step 2: Upload the File

This second step is to upload the file. You use the values returned in Step 1.

This example posts a file test.txt that resides in the local directory.

Example curl Command

```
curl -v -F "key=<key>" \ -F "AWSAccessKeyId=<AWSAccessKeyId>" \ -F
"Policy=<Policy>" \ -F "Signature=<Signature>" \ -F
"file=@test.txt" \ <url>
```

Using REST API to Run a Search

The REST API supports Security Analytics Activity Search index searches. For information about search, see "Getting Started with Activity Search" on page 57.

Request

/api/v1/xdr/usearch/search

HTTP Method: POST

Attributes

Attribute	Description
index	Name of index that you want to perform a search on. Valid values: `iocmatch*`, `dga*`, `threat_bulletin*`, `actor*`, `campaign*`, `ttp*`, `vulnerability*`, `alert_trigger_records*`, `forensic*`, `asset*`.
fields	A list of fields to return in the search results. The online help for each Activity search page has a reference table of the field names for the particular search index.
filters	A list of filter conditions.
query_string	Search query in either of these formats: keyword or field-based. **Note:** The forensic search index supports only keyword searches.
time_range	Event time range.

Example curl Command

```
curl -v -X POST
'https://api.threatstream.com/api/v1/xdr/usearch/search/' -H
'Authorization: apikey <username>:<api_key>' -H 'Accept:
text/plain' -H 'Content-Type: application/json' -d '{"index":
"actor*", "fields": [ "event_time", "event.dest", "event.src",
"indicator", "age", "itype", "confidence", "severity"], "filters":
```

```
{ "confidence": [ 80, 100 ], "itype": [ "apt_domain", "mal_domain"
] }, "query_string": "zscaler* and 172.XX.XX.0/24 and
(severity=high OR severity=very-high)", "time_range": [ "now-1d",
"now" ]}'
```

Responses

Response Code	Example
200 Success	`{ "hits": { "hits": [{ "_id": "0_1c2e61ee-6858-4e59-903d-3ce2f03fb73a__query_178_1_1_2", "_index": "iocmatch_202105", "_score": null, "_type": "ioc_match", "fields": { "age": ["89"], "confidence": ["100"], "event.dest": ["example.com"], "event.src": ["172.XX.XX.XX"], "event_time": ["2021-05-23T18:30:00+00:00"], "indicator": ["example.com"], "itype": ["mal_domain"], "severity": ["very-high"] }, "sort": [1621794600000] }, [...] }`
500 Error	`Error parsing the return from ElasticSearch, Exception = {}`

Using REST API to Run a Forensics and Retrospective Search

> **Note:** The Retrosearch API `/api/v1/xdr/retrosearch` is deprecated. Use the Search API and turbosearch to launch rapid, efficient searches.

The REST API supports forensics & retrospective search. For information about retrospective search, see Forensics & Retrospective Activity Searches.

There are three steps to getting retrospective search results:

"Step 1: Perform a Retrospective Search" below

"Step 2: Create an Export File for the Job Results" on page 1080

"Step 3: Download the Export File" on page 1081

Step 1: Perform a Retrospective Search

The first step is to create a retrospective search job.

Request

> **Note:** The Retrosearch API `/api/v1/xdr/retrosearch` is deprecated. Use the Search API and turbosearch to launch rapid, efficient searches.

api/v1/xdr/search/jobs/

HTTP Method: POST

Attributes

Attribute	Description
data	Specify a keyword or comma-separated list of keywords.
date_range	Event time range. Specify a start time and end time.

Example curl Command

```
curl -X
'POST' 'https://api.threatstream.com/api/v1/xdr/search/jobs/' \
-H 'Authorization: apikey <username>:<api_key>' \
-H 'accept: application/json' \
```

```
-H 'Content-Type: application/json' \
-d '{"query": eventlog | where sourcetype contains "crowdstrike" or sourcetype contains "edr" | aggr count as cnt by src | sort cnt desc | limit 100,"source": "third_party_mynewapp", "time_range": {"from": 1679777426000,"to": 1680123026000,"timezone": "America/Los_Angeles"}}'
```

After submitting retrospective search, poll search status:

```
curl -X 'GET' 'https://api.threatstream.com/api/v1/xdr/search/jobs/6f5f5c716a8b48e1b2659b5918c1b51f/'
-H 'Authorization: apikey <username>:<api_key>'
-H 'accept: application/json'
```

Responses

Response Code	Example
200 Success	`{ "complete": true, "failedMatches": 0, "indexingComplete": true, "jobid": "job871645947359458", "keyMax": 10000, "metrics": {}, "processedFiles": 2316, "reachKeyMax": false, "reason": "", "resultFiles": "", "scannedEvents": 37069166, "status": "completed", "streamResults": [ ], "totalFiles": 2316, "totalIndexed": 3502, "totalMatches": 3502 }`

Step 2: Create an Export File for the Job Results

The second step is to create an export file for the job results.

Request

/api/v1/xdr/export/createUniversalExport/

HTTP Method: POST

Attributes

Attribute	Description
index	`forensic*`
jobid	The jobid from Step 1. For example: `job871645947359458`
selected_ fields	A comma-separated list of fields selected to be included in the export file.
type	`csv`

Example curl Command

```
curl -X 'POST' \
'https://api.threatstream.com/api/v1/xdr/export/createUniversalExp
ort/' \ -H 'Authorization: apikey <username>:<api_key>' \ -H
'accept: application/json' \ -H 'Content-Type: application/json' \
 -d '{ "index": "forensic*", "jobid": "job871645947359458", "page_
title": "Forensics & Retrospective", "selected_fields": [ "event_
time", "confidence", "event.sourcetype", "event.action",
"event.dest", "event.src", "event.user", "indicator", "itype",
"severity", "source" ], "fetch_size": "100", "limit": "100",
"type": "csv", "name": "retrospective_search_result" }'
```

Responses

Response Code	Example
200 Success	`{ "data": "org_id_1_export_1645953032448.csv", "result": true }`
500 Error	`{ "data": {}, "reason": "Index out of bounds error", "result": "False" }`

Step 3: Download the Export File

The third step is to get a signed URL you can use to download the export file. Note the signed URL has an expiration time. You must download the file before the signed URL expires.

Request

/api/v1/xdr/export/download

HTTP Method: POST

Attributes

Attribute	Description
export_id	The export ID (CSV filename) obtained in Step 2.

Example curl Command

```
curl -X POST \
'https://api.threatstream.com/api/v1/xdr/export/download?export_
id=org_id_XXX_export_XXXXXXX.csv' \ -H 'Authorization: apikey
<username>:<api_key>' \ -H 'accept: text/plain'
```

Responses

Response Code	Example
200 Success	`"https://XXXXX/export/orgid%3D1/dt%3D2022-02-27/org_id_XXX_export_XXXXXXX.csv?response-content-disposition=attachment%3B%20filename%20%3Dretrospective_search_test5.csv&AWSAccessKeyId=[...]&Signature=[...]&Expires=1645956651"`
404	`Unable to get s3_file_name form db - {}`
500 Error	`Error occurred when generate the presigned_url for {}, exception = {}`

Using Alerts (Classic UI)

Anomali alerts automate the detection and response process for security events that meet user-defined conditions. By continuously monitoring large volumes of event data, alerts ensure that relevant security signals trigger notifications and response workflows with minimal manual intervention.

Alert rules define the conditions, schedules, and actions associated with each alert. When triggered, alerts can automatically execute configured actions such as sending email notifications, forwarding events to external systems, or adding matched data to ThreatStream investigations, among several others. An organization can configure a maximum of up to 250 alert rules.

These automated workflows help analysts stay informed about critical events without needing to remain logged in to the platform, enabling efficient monitoring and investigation.

> **Note:** Any alert action will return the top 25,000 aggregated search results and 50,000 non-aggregated search results.

Overview

To set up an alert, on the Anomali menu, navigate to **Security Analytics** > **Manage** > **Alerts**.

Alert Rule Types

Event Search alerts are simply specific event search queries run on a schedule. You configure Event Search alerts when you want an automated action to dispatch results for standard queries to email recipients, syslog receivers, third parties, or the Security Analytics Activity alerts index.

Alert Filters

You can use a saved search or or specify filter expressions to narrow the conditions that trigger alerts when matched. Filter expressions follow the same conventions as Activity search filters.

Alert Actions

You can configure one or more of the following actions for each rule:

- **List on Activity Page**: Add to search index used for the **Activity > Alerts** page.
- **Send Email**: Triggered alerts send email notifications, based on the configured alert schedule. The system sends the email through the AWS Simple Email Service (SES).
- **Forward Syslog**: Forward the matched events to a specified Syslog destination.

> **Note:** Only secure Syslog is supported. When you set up the connection to the destination Syslog server in the Anomali Security Analytics configuration, you specify the remote server external IP address and listening port, and you are prompted to upload the destination server CA certificate (cert.pem). The maximum size for the certificate file is 24 KB.
>
> Contact your Syslog server administrator to make them aware of the requirements, and to obtain the external IP address, listening port number, and cert.pem file you need to complete the configuration on the Anomali Security Analytics side.

- **Forward to Splunk HTTP Event Collector**: Forward the matched events to a specified Splunk HEC destination. Anomali recommends forwarding alerts to Splunk HEC instead of Splunk syslog TCP input.
- **Webhook**: Forward matched events to a third-party service as a customizable JSON payload via an HTTP POST request. For example, you can use a webhook connection to create a ServiceNow ticket after Security Analytics triggers an alert. To set up a webhook connection:
  - Navigate to **Manage** > **Alerts**.
  - Click **Create Alert**.
  - Select the **Alert Source**: Enter an alert name, description, and select the source of the alert. Currently, webhook actions are triggered only for search alerts.
  - Set the following alert specifications:

  - Search type — Saved search or Custom search
  - Event time range
  - Alert schedule
  - Alert trigger condition
  - Throttle conditions
- Set the alert actions: Add a new webhook alert action, by providing the following information:
  - Select **Webhook** as the action.
  - Specify the **URL** to send the JSON payload through an HTTP POST request.
  - (Optional) Provide an **Authorization Header**.
  - (Optional) Provide any **Custom Header**.
  - Enter the **Payload** the webhook will share in JSON format.
  - Select **Trigger for every match** (unchecked by default) to make a single call for every alert trigger and for the third-party service to send one webhook call for each match in the results set.
  - Click **Save**.
- Click **Save** to finish creating the alert.
- Here's an example of the JSON payload customization:

The user configures an alert for the search query: `eventlog | fields event_time, sourcetype, action, user | limit 10`

You can configure the JSON payload while setting up the webhook connection as follows:

- Option 1: **Trigger for every match** unselected

```
{
    "alert": "My event log alert",
    "time": "{{events[0].event_time}}",          # Get the value of the field 'event_time' from the first record
    "source_type": "{{events[1].sourcetype}}",     # Get the value of the field 'sourcetype' from the second record
    "user": "{{events[2].user}}"                 # Get the value of the field 'user' from the third record
}
```

- Option 2: **Trigger for every match** selected (that is, a separate call per trigger)

```
{
    "alert": "My event log alert",
    "time": "{{event.event_time}}",
    "source_type": "{{event.sourcetype}}",
    "user": "{{event.user}}"
}
```

- **Forward to Azure**: Forward the matched events to an Azure Sentinel instance.

> **Note:** To configure forwarding the matched events to an Azure Sentinel instance, make sure that the following prerequisites are met:
>
> - A Microsoft Entra application which is used for authentication is created and its secret is generated.
> - A Data Collection Endpoint (DCE) is created.
> - A new table in the Log Analytics workspace is created.
> - A Data Collection Rule (DCR) is created and a sample alert JSON to create a schema is created.

Example of an alert JSON (not all possible fields are specified):


```
{"action":"writeval","aggregated_
query":false,"alert_batch_id":"41","alert_rule_
name":"dy_azure_test","alert_time":"2024-07-
20T15:25:26.281233Z","aql_query":"eventlog |
limit
10","day":"20","dcid":"1","dest":"","event_
meta_id":7435887944,"event_
time":1720000032,"hit_
count":"10","hour":"15","http_referrer":"http
ref","match_records_time_window":["2024-07-
20T14:25:00Z","2024-07-20T15:25:00Z"],"match_
type":"event_search","minute":"00-0","rule_
type":"event_search","sourcetype":"carbon_
black","src":"WIN81-VM","trigger_condition":
{"operator":"gt","value":0},"url":"","user":""}
```


- The Microsoft Entra application is assigned permissions to use the Data Collection Rule.

For more information, see https://learn.microsoft.com/en-us/azure/azure-monitor/logs/tutorial-logs-ingestion-portal.

Once the alert is triggered and the alert JSON is sent to Azure, it can be found in the Azure table. Azure accepts up to 1000 alerts.

The fields absent from the schema will not be ingested. If you need to update the schema, you can do it in Azure and wait until the changes are applied.

Configure an Event Search Alert

Event Search alerts are simply specific event search queries run on a schedule. You configure Event Search alerts when you want an automated action to dispatch results for standard queries to email recipients, syslog receivers, the Security Analytics Activity alerts index, or a third-party via HTTP POST. The alert action is triggered only when the event search result set is not empty.

To configure an alert:

1. Navigate to **Manage** > **Alerts**.
2. Click **Create Alert** to start the rule wizard.
3. Configure the Source settings described in the following table.

Setting	Description
Alert name	Type a name that facilitates configuration management. This name also appears in Activity search for alerts. Only ASCII characters are allowed for the configuration name.
Description	Type a description to help other administrators understand the purpose of the rule.
Source	Select **Search**.

4. Click **Next** to go to the alert specifications page.
5. Complete the settings described in the following table.

Setting	Description
Saved Search or Custom	▪ **Saved Search**: Select a saved search. It must be an Event Search saved search. ▪ **Custom**: Specify a valid AQL search expression. If you use a saved search, changes you subsequently make to the saved search affect the alert. If you want to use a saved search with its current AQL syntax and have the alert not subject to subsequent changes to the saved search, use the **Copy** button to copy the AQL syntax to the clipboard, click **Custom**, and then paste the content in the Query box. **Tip**: In most cases, you want to use tightly refined queries (including sort and limit operators) to reduce alert noise.
Query	If you selected **Custom**, paste valid AQL syntax in the query box.

Setting	Description
Event Time Range	Specify a time range for the query. The time range should be a relative time expression since the alert will be run on a schedule. The event time range you configure will be relative to the time the alert is run. Possible values include: ▪ **Previous hour**: includes events having timestamps in the hour before the alert is run ▪ **Previous 4 hours**: includes events having timestamps in the past 4 hours before the alert is run ▪ **Previous 6 hours**: includes events having timestamps in the past 6 hours before the alert is run ▪ **Previous day**: includes events having timestamps in the past day before the alert is run ▪ **Custom Time Range**: includes events having timestamps within the specified custom time range. ◦ **From**: select the start time of the range, either in minutes, hours, days, or weeks. ◦ **To**: select the end time of the range, either resolving to the current time or up to the selected number of minutes, hours, days, or weeks ago.

Setting	Description
Alert Schedule	Specify a frequency for the rule to be evaluated. Possible alert schedules include: ▪ **Every hour** ▪ **Every 4 hours** ▪ **Every 6 hours** ▪ **Every day** ▪ **Every week** ▪ **Custom schedule**: Run the schedule after a specified number of minutes, hours, or days ▪ **Cron schedule**: Schedule alerts using cron expressions ◦ **Default**: Schedule a cron job to run either every: • minute • hour: runs after the specified number of minutes past the hour • day: runs every day at the specified time (in 24-hour format) • week: runs only on the specified day of the week at the specified time (in 24-hour format) • month: runs on the specified day of the month (between 1-31) at the specified time (in 24-hour format) ◦ **Cron**: Schedule the cron job using a valid cron expression. For example, using `8 18 14 * *`

Setting	Description
	as your cron expression runs the job at 6:08 PM on day 14 of the month.

Setting	Description
Alert if number of results	Specify a condition that triggers the alert: ■ **Is greater than**: Number of rows in the result set is higher than the number specified in the rule. ■ **Is less than**: Number of rows in the result set is lower than the number specified in the rule. ■ **Is equal to**: Number of rows in the result set is exactly the number specified in the rule. ■ **Is not equal to**: Number of rows in the result set is any number of rows except the number of rows specified in the rule. ■ **Is greater than or equal to**: Number of rows in the result set is higher than or equal to the number specified in the rule. ■ **Is less than or equal to**: Number of rows in the result set is lower than or equal to the number specified in the rule. ■ **Increases by**: When the query was run for the current interval, the number of rows in the result set increased by at least the specified number compared with the number of rows in the result set for the preceding period. ■ **Decreases by**: When the query was run for the current interval, the number of rows in the result set decreased by at least the specified number compared with the number of rows in the result set for the preceding period. ■ **Custom Query**: Enter a alert trigger condition as a custom query to append to the main query at the top (Saved Search or Custom). For example, if:

Setting	Description
	◦ Main Query: `eventlog | limit 10` ◦ Custom Query: `where severity="low"` (or `| where severity="low"`) then the final query becomes: `eventlog | limit 10 | where severity="low"`
Throttle	Select this option to prevent the same event search alert from being triggered repeatedly within a specific time window. If you select this option, specify the following settings: ▪ **Throttle Results Containing**: Specify one or several fields for which the event must contain the same values in order for throttling to be enabled. By default, fields are from the eventlog table but you can specify your custom fields as well. For this, type the name of a custom field, and then press Enter. ▪ **Throttle for**: Specify the time window during which the throttling should be enabled for selected results. **Note**: Throttling time window must exceed the alert schedule. For example, if an alert triggers when a user fails to log in more than 5 times within 10 minutes, you can throttle subsequent alerts for the same user for 1 hour.

6. Click **Next** to go to the Action page.

7. Click the Plus icon ( ) and then select and configure a rule action.

You can configure multiple actions. The settings for actions are described in the following table.

Action	Setting	Description
List on Activity Page	List on Activity Page	Add to search index used for the **Activity** > **Alerts** page. When the alert is triggered, a new entry is added to the Alerts activity search index. From the Activity page, you can find Event Search alerts by filtering on rule name. Click the Details icon for the alert to issue an Event Search with the alert rule search criteria.
Send Email	To	Type or select one or more email addresses.
	Subject	Specify an email subject line. The default value uses the `$alert.name$` variable to set the subject to the rule name.
	Priority	Lowest, Low, Medium, High, Highest
	Message	Specify a message body. The default uses the `$alert.name$` variable to form a message that identifies the rule that triggered the alert. The message body shows the alert rule name, the search string, event search time range, time the alert was triggered, and trigger condition details. The alert message includes a maximum of 1,000 rows.

Action	Setting	Description
Forward Syslog	Format	Format in which the alert will be sent. For Syslog or Splunk, select JSON. For ArcSight ESM or QRadar, select CEF. The alert message includes a maximum of 100 rows.
	Facility	Select a syslog local facility for the messages. The facility value is only used when CEF is selected. **Note:** The facility value is a component of the priority value added to the beginning of the message in conformance with RFC 5424. Priority value is a combination of the facility and severity values. For Security Analytics, the severity value is always 6 (info). Therefore, with CEF format, you can use the facility value to forward Security Analytics alerts to facility-based locations specified on the remote server.
	Address	Host name or external IP address for the remote syslog server to which the alerts will be sent. Ask your Syslog server administrator for the external IP address. The syslog server must be configured to allow syslog communication from Security Analytics over the Internet. Only syslog over TCP is supported.
	Port	Listening port for the specified host. Ask your Syslog server administrator for the correct port.
	CA certs	Only secure Syslog is supported. Click **Browse** and upload the destination server CA certificate (ca.pem file) provided by your Syslog server administrator. The maximum size for the certificate file is 24 KB.

Action	Setting	Description
	Output Raw Only	If checked, forwards only the raw event output of the alert, without its metadata fields. Use this option when the server truncates alerts that exceed the acceptable length.

Action	Setting	Description
Forward to Splunk HTTP Event Collector	Format	Format in which the alert will be sent: JSON or CEF. The alert message includes a maximum of 1,000 rows.
	Splunk Host	If your Splunk instance is Splunk Enterprise, specify the fully qualified domain name (FQDN) or IP address for the Splunk host. If your Splunk instance is Splunk Cloud, specify `http-inputs-<host>.splunkcloud.com`, where <host> is the Splunk Cloud Platform instance that runs HEC. For example, `http-inputs-anomali.splunkcloud.com`. Refer to Splunk documentation for more information.
	Splunk Port	Specify the port that is configured in the HTTP Port Number field of Global Settings of Splunk HTTP Event Collector. The default in both Splunk HEC and the Security Analytics alert configuration form is 8088. **Note**: The port for Splunk HEC is typically different from the port for the Splunk dashboard. For example, a Splunk instance can be set up to have the Splunk dashboard accessible at 192.168.10.124:8000 and the Splunk HEC port configured to accept data on port 8088.
	Splunk Token	Copy the token value expected by the Splunk HTTP Event Collector. Refer to "Forwarding Alerts from Anomali Security Analytics to Splunk" in the *Anomali Link (for Splunk) Installation Guide* for an illustrated example.

Action	Setting	Description
	Output Raw Only	If checked, forwards only the raw event output of the alert, without its metadata fields. Use this option when the server truncates alerts that exceed the acceptable length.
	HTTPS Enabled	Select this option if HTTPS is enabled on the Splunk HTTP Event Collector.
Webhook	URL	Specify the URL of a third party to which the matched events will be sent via an HTTP POST request. The third party will receive the matched events as a JSON payload.
Forward to Azure	Directory (Tenant) ID	Copy the Directory (Tenant) ID value in the Microsoft Entra application settings.
	Application (Client) ID	Copy the Application (Client) ID value in the Microsoft Entra application settings.
	Client Secret	Copy the generated secret for the Microsoft Entra application
	Client Collection Endpoint	Copy the Logs Ingestion URL value in Data collection endpoint settings.
	Data Collection Rule	Copy the Immutable Id value in Data collection rule settings.
	Data Collection Rule Stream Name	Copy the stream name in Data collection rule settings (JSON View). It represents the table in which the forwarded alerts will be stored. The stream name string includes the table name.
	Output Raw Only	If checked, forwards only the raw event output of the alert, without its metadata fields. Use this option when the server truncates alerts that exceed the acceptable length.

Action	Setting	Description
Add to Alert Triage	Status	Required. Status that the creator of the alert wants to assign to the triggered alert. New: A new rule is configured. Open: A configured rule is still valid and isn't completed. In Progress: A configured rule is currently
	Risk Score	Required. An integer (1–100) that represents the risk associated with the triggered alert.
	Severity	Required. Indicates the severity of the triggered alert. Possible values: Critical, High, Medium, Low.
	Owner	Required. The email address of the owner of the triggered alert, which can be either the creator's email or the analyst that will address this alert. **Note:** You need permissions to add alert rules. See SSO and Role Management to understand who can create rules.
	Assignee	Required. The email address to which the alert action is assigned, typically a security analyst.

Action	Setting	Description
	Add MITRE Association	Optional. Add an association to the MITRE framework to send enhanced information about the event that triggers the alert and its impact. **Domain**: Select one of the MITRE ATT&CK domains from Enterprise, ICS, and Mobile, depending on the MITRE version. **Tactics**: Specify the type of tactics involved — collection, command and control, or credential access. **Techniques**: Specify the type of technique involved. For example, the `T1003` technique refers to credential dumping that is used to extract login credentials from compromised systems.
	Add Entities	Optional. Add information about event, asset, and identity entities as a JSON string. Here, the values are populated using the first row of the search results. For example, `event entity` can be `{"name": "<<hostname>>", "ip": "<<src_ip>>", "source": "<<source>>"}`.`

Action	Setting	Description
Forward to AWS S3	S3 Bucket	Required. URI of the S3 bucket to which the alert will forward the alert payload. Example: `s3://test_bucket/folderA/...`
	Access Key	Required. Enter the AWS S3 Access key of the S3 bucket.
	Secret Key	Required. Enter the AWS S3 Secret Access Key.
	Output Format	Required. Select an output format for the alert payload, either JSON or CEF.
	Output Raw Only	Optional. If selected, forwards only the raw event output of the alert, without its metadata fields.

8. Click **Save**.

Modify an Alert Configuration

	In the Actions column, click the Edit icon to modify an alert configuration.

Clone an Alert Configuration

	In the Actions column, click the Clone icon to create an editable copy of an alert configuration.

Delete an Alert Configuration

	In the Actions column, click the Delete icon to delete an alert configuration.

Review Alert Rule Details

	In the Action column, click the Review icon to see rule configuration details and a history of alerts generated by the rule.