

Important Update on Recorded Future Intelligence

Effective February 10, 2023

As part of Anomali's ongoing efforts to improve its infrastructure and better serve its customers, the existing private **Recorded Future** feed has been removed from the APP Store, and the new premium feed **Recorded Future - Default Risk List** has been added instead. As a result of this, all customers using the Recorded Future feed have been migrated to the new feed.

The Recorded Future - Default Risk List feed brings several improvements, including enhanced performance and improved accuracy. The data in the Recorded Future - Default Risk List feed is identical to what the customers were receiving via the private Recorded Future feed. The new feed can be activated with the API key from the existing private Recorded Future feed.

If you have any additional questions or concerns, contact your Customer Success representative.

FAQ

1. **Why was this change made?**

The change to the new "Recorded Future - Default Risk List" intelligence feed was made in order to transition to a more efficient channel-based feed. By moving to a channel-based feed, we believe that we will be able to offer enhanced performance and improved accuracy to better serve the needs of our customers.

2. **Will I lose any intelligence when I migrate to this new channel feed?**

No, you will not lose any intelligence when you migrate to the new channel-based feed. The new feed has an identical set of Indicators of Compromise (IOCs) as your current private RF feed. Additionally, we have backfilled the past 3 years' worth of data, ensuring that you have access to the same intelligence that you have been receiving. Rest assured that we have taken all necessary steps to ensure that the transition to the new feed is seamless and does not result in any loss of intelligence for our customers.

3. **Do I need to make any other changes on my side?**

It depends on how you are using the Recorded Futures feed_id in your saved searches and rules. If your saved searches and rules use the feed_id as a filtering parameter, then you will need to update those saved searches and rules to use "trusted_circle_id=396" instead. This will ensure that your saved searches and rules continue to work as expected after the change.

If you don't have the Recorded Futures feed_id as a parameter in any of your saved searches or rules, then no changes are necessary on your side.

It's always a good idea to double-check and verify that your saved searches and rules are working as expected after making changes like this, to ensure that you are still receiving the information that you need.

4. **What is the confidence weighting for this Recorded Future (RF) feed?**

The confidence weighting for the Recorded Future feed is 70% RF & 30% Anomali Macula to reduce false positives.

5. **What if I want to use only Recorded Future-provided confidence to filter the data? How do I do that with Recorded Future (RF) confidence weightage set to 70%?**

Using the search filter "source_reported_confidence" in combination with "trusted_circle_id" will return filtered Recorded Future Results based on the confidence the source (Recorded Future) has set.

e.g. IOCs from RF channel feed where confidence set by RF is >80

trusted_circle_id = 396 and source_reported_confidence > 80

6. **What if I want to use Anomali confidence scoring instead of Recorded Future-provided confidence to filter the data?**

You can use the "retina_confidence" criteria in the search filter for IP, Domain & URL IOCs to filter based on Anomali confidence scoring. Note that Macula doesn't score the Hash, Email & String IOCs, so for those retina_confidence=-1.

e.g. IF you want to get IPs from the RF channel where macula confidence >80

trusted_circle_id = 396 AND type = ip and retina_confidence > 80