Cisco XDR Known Issues

Contents

Introduction

Known Issues

- Incidents
- Investigations
- Control Center
- Cisco Integrations
- Cisco Identity Intelligence
- Third-Party-Integrations
- Assets
- XDR Automate
- Appliances/Sensors
- Secure Client
- XDR Forensics
- XDR-Analytics
- Orbital

Resolved Issues

Introduction

This article documents currently known technical issues for Cisco XDR.

Technical issues can be acknowledged by Cisco, under review, pending resolution, or deemed working as expected.

Known Issues

Incidents

No known issues for this XDR functionality at this time.

Investigations

No known issues for this XDR functionality at this time.

Control Center

No known issues for this XDR functionality at this time.

Cisco Integrations

1. Cisco XDR - Cisco Secure Firewall Full Integration

Details: To ensure seamless integration between Cisco Defense Orchestrator (CDO), Security Services Exchange (SSX), and Security Analytics and Logging (SAL), manual mapping is required. This process involves contacting Cisco TAC to perform the necessary configurations and mappings.

Workaround: Contact TAC in order to assist in linking the relevant accounts and ensuring proper integration of the systems.

Expected Resolution: TBD

Cisco Identity Intelligence

1. A small number of customers have duplicate Cisco Identity Intelligence modules

Status: Issue Identified and Pending Resolution

Details: Some customers were accidentally provisioned a second module when Cisco Identity Intelligence was brought into the XDR product. Affected customers will now show duplicate CII sources in Asset Insights, and duplicate CII automation targets.

Workaround:N/A

Next Steps: Engineering investigating causes/solution

Resolution: The fix for the creation of duplicates will be released in *version 2.57*. A fix for the existing duplicates is being investigated.

Third-Party-Integrations

1. Missing Cloud Provider Value for OCI Flows in XDR-A Event Viewer

Status: Issue Identified and Pending Resolution

Details: The cloud provider column in the XDR-A Event Viewer is currently blank for flows ingested from OCI.

Workaround: Users can still filter for these flows by manually typing "OCI" in the table filter.

Next Steps: Cisco is working on implementing a fix for this issue.

Resolution: February 2026

Assets

No known issues for this XDR functionality at this time.

XDR Automate

No known issues for this XDR functionality at this time.

Appliances/Sensors

No known issues for this XDR functionality at this time.

Secure Client

In order to consult the issues for Secure Client, please refer to the article.

XDR Forensics

1.- Performing XDR Forensics actions when asset in XDR Incident has not resolved but has Forensics module installed

Status: Under investigation

Details:XDR Forensics depends on assets to be resolved within an XDR Incident before forensic actions can be executed on an asset from an Incident's Evidence tab. If Cisco XDR is unable to resolve an asset in an XDR Incident, this will preventXDR Forensics evidence acquisition from being available from the Incident.

Workaround: Pivot from Cisco XDR console to XDR Forensics to perform the forensic action.On the left navigation menu of Cisco XDR, click Investigate > Forensics

In XDR Forensics, click Assets on the left navigation menu, select the appropriate asset and acquire evidence and/or desired action.Select the appropriate case from the drop-down menu so that this is automatically associated with the XDR Incident.

Next Steps: TBD

Resolution: TBD

Tracking CDETS:Cisco bug ID CSCwr69610

2.- XDR Forensics operations can be blocked by Cisco Secure Endpoint or other endpoint security solution's endpoint isolation response action.

Status: Under investigation

Details:XDR Forensics can be blocked by Cisco Secure Endpoint, EDR or other endpoint security tool's isolation enforcement.Ensure that the appropriate exclusions and allow lists for XDR Forensics are configured to the endpoint security tool.

Workaround:

(Example based on Cisco Secure Endpoint's Isolation Feature, but applies generally to other endpoint security software)

Get the IP addresses

- Perform an nslookup/dig of your XDR Forensics tenant url (can be obtained by pivoting into XDR Forensics and copying the URL from the browser (remove the https, and everything from the first slash to the end)
- Make note of all the IP addresses

Add an Isolation IP Allow list

- In the endpoint security product, for example - Cisco Secure Endpoint, navigate to Outbreak Control > IP Block & Allow Lists

- Select the tab for Isolation IP Allow lists. If you already have one you can update it, otherwise use the "Create IP List" button to add a new one
- Give it a name and description then add the IPs from the previous step
- Save the list

Add Allow List to Policy

- Navigate to Cisco Secure Endpoint’s Management > Policies
- Choose the policy you want to update and click to edit
- Navigate to Advanced Settings > Endpoint Isolation
- (If necessary) Select the Allow Endpoint Isolation checkbox
- In the Isolation IP Allow Lists, choose the List(s) you want to include
- Click Save

Next Steps: TBD

Resolution: TBD

Tracking CDETS: Cisco bug ID CSCwr69614

3. - Modifying the default role permissions in XDR Forensics can cause non-intuitive errors in the XDR Incident and XDR Forensics integration for users.

Status: Under Investigation

Details: In XDR Release 2.5.6 (Released on 12-17-2025), XDR Forensics Global Admins can now modify the user role permissions in XDR Forensics for more granular control. However, modification of permissions related to core acquisition, InterACT remote shell and case functions will result in permissions errors in the integration between XDR Incident and XDR Forensics. For example, a user with a role that is modified to remove remote shell permission, will still see the remote shell action option in the XDR UI, but will be prevented from establishing the remote shell session. While documented in XDR Forensics release notes, this error due to permissions restriction may not be intuitive to a user on the XDR console.

Workaround:XDR Forensic global admins must validate the modified permissions with intended user role functionality before implementing.

Next Steps: TBD

Resolution: TBD

XDR-Analytics

1. - Several IP addresses and/or multiple host names can get associated with a single device name in XDR-A

Status: Un-Resolved / Postponed

Details: Several active IP addresses can get associated with a single device within the SNA/XDR-A Portal. This can include both NVM and non-NVM devices. Some devices also have multiple

hostnames. Based on the current implementation, the registration of devices could result in a device having more than one IP address (location). Some of these IP addresses can be from the user's home network and may collide with IP addresses in the organization's network.

Workaround: There is no work around for this issue at this time, and the issue still exists in the current architecture. There are hopes that this issue may be better addressed in the future, once new architecture is implemented which will allow for network activities from both sources ONA and NVM to be normalized to OCSF and brought together. There have also been updates to the expiry of IP Devices which are seen to be associated with a new hostname to accelerate expiry.

Next Steps: N/A

Resolution: Future / TBD

Tracking CDETs: Cisco bug ID CSCwo67299

Orbital

1. Deployment limitation for Secure Endpoint essential customers

Status: Issue Identified and Pending Resolution

Details: In the Admin > Integrations Tabs the Secure Endpoint "Enable" Link is broken. Once we hit the enable button, it is redirecting to the Threat Response page and it loops to the XDR org selector page instead of going to the Secure Endpoint Console.

Workaround: Integration can be performed from the Cisco Secure Endpoint Portal

Next Steps: Cisco is working to implement the fix for this issue

Expected Resolution: TBD

Resolved Issues

1.- Cisco XDR - Cisco Secure Endpoint integration link not working on Cisco XDR Portal

Status: Issue Identified and Pending Resolution

Details: XDR customers of any tier who also have Secure Endpoint essentials may be prevented from installing Orbital, since the Secure Endpoint connector will actively disable Orbital. To resolve this conflict, please reach out to TAC.

Workaround: N/A

Next Steps: Cisco is working to implement the fix for this issue

Expected Resolution: This issue has been resolved.

2.- XDR Automate Incident Automation Rules unexpectedly stop running

Status: Issue Identified and Pending Resolution

Details: Incident Automation Rules powered by workflows and triggers unexpectedly stop running. This is not indicated in the XDR User Interface, except when reviewing the metrics for ***Workflows Run Over Time.*** When doing so, customers will see reduced or zero workflows run, depending on how long

the issue has been ongoing.

Next Steps: Cisco has identified this as an issue within the XDR backend and is working to resolve it. Cisco also plans to implement additional monitoring and state-tracking features to avoid this issue from occurring in the future.

Workaround: Disable and Re-enable the rule to kick off a restart of the workflow rule triggering and processing.

Expected Resolution: Resolved.

3. - Cisco XDR-Analytics - ONA installation failure in Virtual Environments with an error indicating "***checksum verification failed***"

Status: Issue Identified and Pending Resolution

Details: When deploying a ONA sensor in a Virtual Environment, the ISO fails to complete the install process and errors out.

Workaround: Install Ubuntu Server 24.04 independently with the Ubuntu ISO and refer to the advanced install steps to run ONA as a service. Use the 7.0 U2 compatibility

Next Steps: N/A

Resolution: This issue has been resolved in the latest build of the ONA Sensor

4.-MTTR tile on the Control Center shows inaccurate numbers for incidents that have been resolved using one of the new states such as "Closed: False Positive", "Closed: Confirmed Threat" or other.

Status: Issue Identified and Pending Resolution

Details: New incident states have been introduced on Jan 15th and the tile does not take those states into consideration. The new resolution states are interpreted as work-in-progress, so even if that incident has been closed using one of the new states, it is accounted for as work in progress.

Workaround: None

Next Steps: None

Expected Resolution: Resolved

If you need to contact Cisco Support, refer to the instructions provided in this link.