Cisco Crosswork Cloud User Guide

First Published: 2020-01-23

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

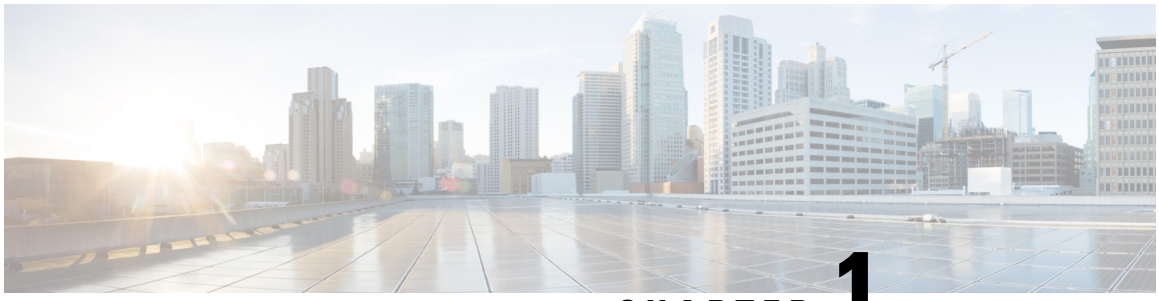
Short Description

CONTENTS

?

PART I

About Crosswork Cloud



CHAPTER 1

About Crosswork Cloud External Routing Analytics

About Crosswork Cloud Network Insights

Your network can be a complex and often times unpredictable environment. Routing events that are caused by automated systems, malicious attacks, or simply operational errors can have unforeseen effects on network services. Routing protocol event information can be difficult to comprehend when not organized, analyzed, and displayed logically.

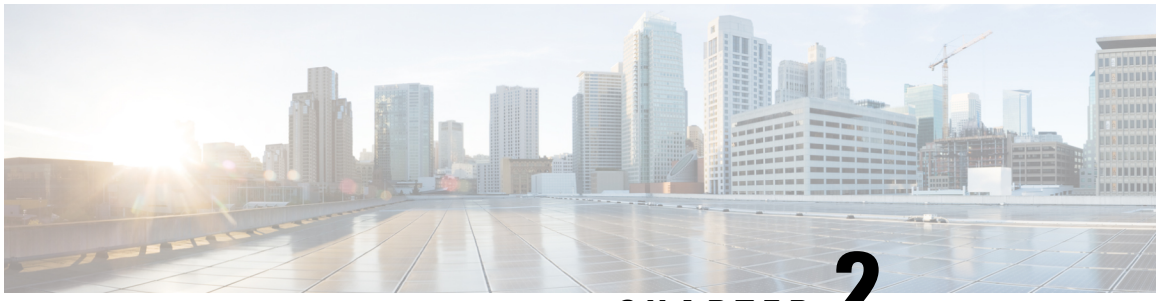
Crosswork Cloud Network Insights is a SaaS application that provides rich analysis, visualization, and alerting on actionable network events. Crosswork Cloud Network Insights operates as a hosted service and helps you assess the routing health of your network. Crosswork Cloud Network Insights provides you with the information you need to determine the stability of your networks and potential risks to your IP routing assets. Crosswork Cloud Network Insights aggregates global and local routing information and identifies the source of anomalies based on a consensus of the routing databases. You can track live and historical activity of your own global BGP and IP information. You can also quickly and easily investigate other entities that might be the cause of issues based on the information provided by the platform

The service provides a secure and low-risk method of collecting route information at a global scale.

Crosswork Cloud Network Insights Tools

In addition to monitoring routing information, Crosswork Cloud Network Insights provides a set of tools to help validate ROA information and graphically visualize AS paths:

- Path Topology—Provides a topology view of all peer, transit, and origin ASN that are advertised in AS paths for a prefix. For more information, see View Prefix Topology.
- Route Origin Validation—Compares ROA information against BGP updates. If the ROA information does not match the data retrieved from a BGP update, it is considered a violation. By default, the tool displays all prefix ROAs in violation (ROA Status filter is set to **Invalid**). For more information, see Validate Route Origin Information.



CHAPTER 2

About Crosswork Cloud Traffic Analysis

About Traffic Analysis

Crosswork Cloud Traffic Analysis provides helpful insight about how traffic is affecting your network. By providing traffic statistics on the ASNs, prefixes, and interfaces in your network, Crosswork Cloud Traffic Analysis can give you real-time information on how your devices are performing.

With Crosswork Cloud Traffic Analysis, you can help prevent and address network edge congestion as well as answer the following questions:

- Can we quickly manage congestion at network edge?
- Can we proactively identify network edge congestion? What small changes could help network edge congestion?
- How do IP Routing tables relate to traffic flow in congested devices?
- Who should we peer with and what changes should we make to achieve a Peering Traffic load balance?
- What is the impact of moving traffic between edge devices?

Crosswork Cloud Traffic Analysis aggregates traffic flow data across multiple devices, giving operators a view of the traffic matrix across the whole network. It adds critical context to observed traffic flows based on the existing rich data sets of external routing data from the Crosswork Cloud Network Insights service. This allows operators to gain a deeper understanding of the origins of traffic flows on their networks, as well as the impacts of changes in external routing state and policy. By effectively extracting and managing huge amounts of data, operators can rapidly address and even proactively avoid disrupting events and impending security threats.

Cisco Crosswork Cloud Traffic Analysis also provides actionable recommendations for optimizing traffic at congested network edges. As the number of peering points expand in today's distributed networks, delivering this end-to-end traffic visibility at scale becomes a critical requirement for effective network optimization. This visibility allows network operators to drive manual or automated changes that are clear and easy to implement based on defined policies – throughout the network.

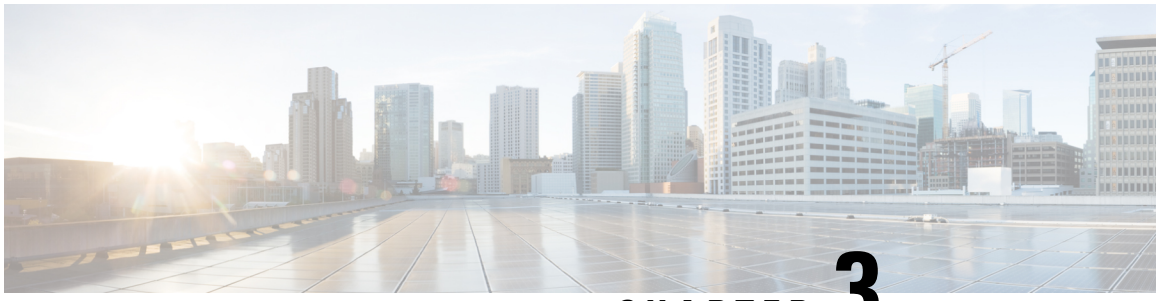
View Traffic Information

- View Device Traffic Details

- View Interface Traffic Details
- View ASN Traffic Details
- View Prefix Traffic Details

Use Crosswork Cloud Traffic Analysis Tools

- Optimize Interface Utilization—Provides a suggested list of prefixes where traffic from overutilized edge interfaces can be diverted to underutilized edge interfaces to normalize overall utilization.
- Visually Compare Traffic—Compares traffic between like objects such as ASNs, prefixes, devices, and interfaces.
- Traffic Drilldown—Allows you to easily view interface capacity and what traffic sources are contributing to it.
- Peer Prospecting—Shows you on which peer ASNs large amounts of traffic are being transmitted and received. It helps you select a current peer and quickly see other peers to which you could move traffic.



CHAPTER 3

About Crosswork Cloud Trust Insights

About Trust Insights

Crosswork Cloud Trust Insights provides a way to protect and test the integrity of Cisco IOS XR devices on your network. Crosswork Cloud Trust Insights gathers secure measurements and proves that the data was collected at a certain time, which allows you to measure, verify, and audit the integrity of your network. Crosswork Cloud Trust Insights automatically interprets and verifies the integrity of Known-Good-Values (KGVs) measurements from IOS XR routers. This provides a unique visibility into hardware and software integrity and trustworthy status of production routers in your environment.

Crosswork Cloud Trust Insights helps you understand what is true on your network now and what was true in the past. It also helps you answer the following questions:

- How do I know that my router is running the software I want it to be running?
- How can I track what hardware and software has changed?
- How do I know if someone has modified the hardware or software running in my network?
- How can I prove where and when critical security updates were applied and are currently active?
- How can I be sure that the running software was built by Cisco?
- How can I verify what hardware and software was running in a particular date in the past?
- How can I prove that my systems are running compliant hardware and software?

Data Used by Trust Insights

In order to verify and prove the integrity of the hardware and software in your network, Crosswork Cloud Trust Insights uses the following data:

- Known Good Values (KGVs)—Cisco produces and publishes KGVs for its hardware and software products. The KGV.json file is signed by Cisco and contains measurements for various components such as boot integrity visibility, boot0 image measurements, boot OS image measurements, and running image file measurements. KGVs provide a standard of known, good values which test validity.
- Signed evidence dossiers from IOS XR devices—New features in IOS XR allow the ability to generate a dossier that contains trust information about the running hardware and software such as the operation status, inventor, and hardware, boot, and run-time integrity. Crosswork Data Gateway gathers the dossier and forwards it to Trust Insights.

How Trust Information is Gathered from Devices

The following steps explain the process by which Crosswork Cloud Trust Insights gets the trust dossier from devices.

1. Crosswork Data Gateway connects to Crosswork Cloud (HTTPS).
2. An administrator adds Crosswork Data Gateway information and devices to Crosswork Cloud Trust Insights.
3. Trust Insights sends Crosswork Data Gateway a list of devices to query.
4. Crosswork Data Gateway logs in to the devices and gathers the trust dossier.
5. Crosswork Data Gateway forwards the trust dossier to Crosswork Cloud Trust Insights.
6. Crosswork Cloud Trust Insights performs verification and analytics.

How Trust Insights Measures Trust

To test and measure trust in your network devices, Crosswork Trust Insights performs the following steps:

- Trust Insights securely request and collects a signed-evidence dossier from IOS XR devices by using the Cisco Crosswork Data Gateway.
- The dossier evidence is verified and added to the timeline of running hardware and software.
- Crosswork Trust Insights compares the data contained in the dossier against KGVs from Cisco for the hardware and software.
- Crosswork Trust Insights displays assured inventory reporting with history and trust visibility for the devices.

What Trust Insights Can Verify

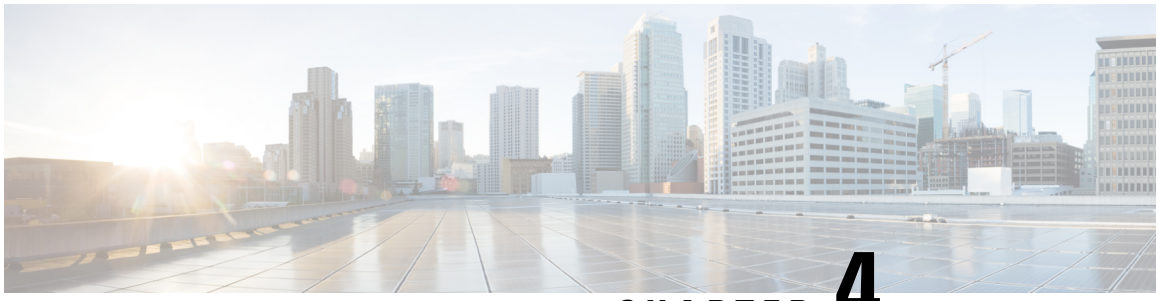
Crosswork Cloud Trust Insights gathers and reports on evidence of software and hardware changes. For example, if you need to apply an SMU to address a security vulnerability on a device, Trust Insights can provide evidence that you're running the correct SMU and that the code you installed has fixed the vulnerability.

Trust Insights cannot:

- Determine if a router is up or down. Trust Insights isn't an operational tool.
- Verify the integrity of any code that Cisco didn't create. If we recognize the data from the operating system or an SMU, we can verify that your devices are running the software you think they are running. However, if we see data that we don't recognize, Trust Insights can’t determine its validity or integrity.

PART II

Get Started with Crosswork Cloud



CHAPTER 4

Log In

Supported Browsers

Crosswork Cloud products are supported on the following browsers:

- Google Chrome 70 or later
- Mozilla Firefox 62 or later

Log In

Note Crosswork Cloud supports the following browsers:

- Google Chrome 70 or later
- Mozilla Firefox 62 or later

To log in to Cisco Crosswork Cloud:

Step 1 In your browser, go to https://crosswork.cisco.com.

Step 2 From the Crosswork Cloud page, click **Login**.

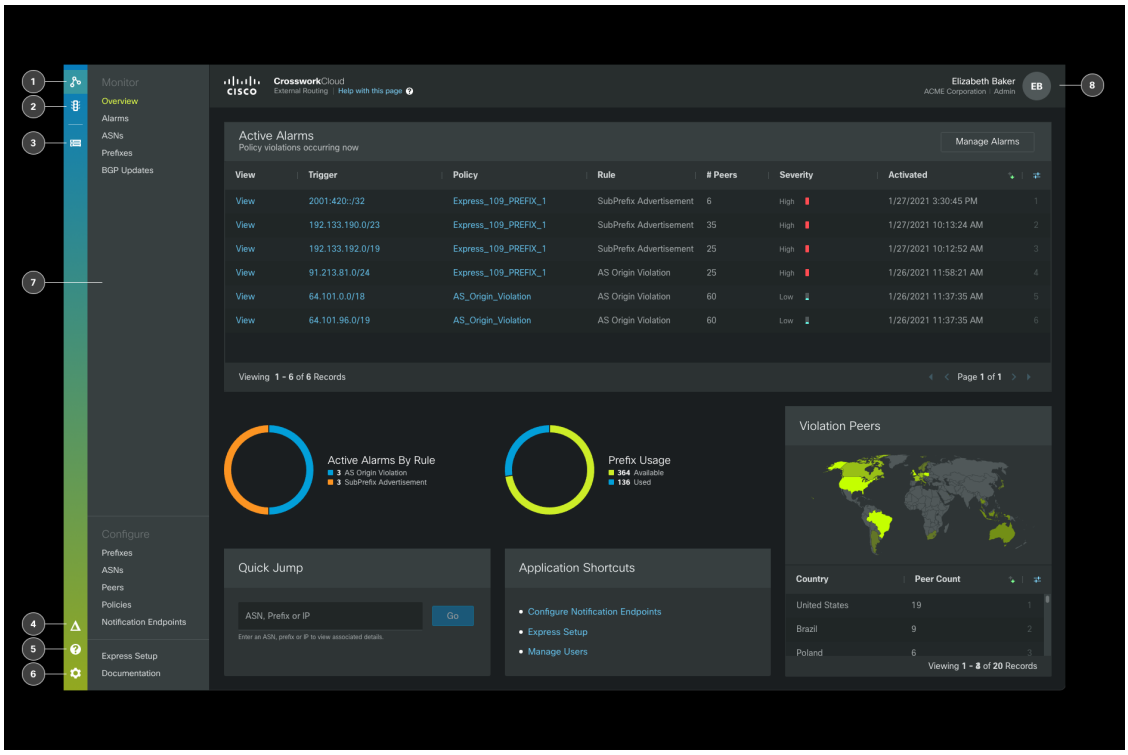
Step 3 Enter your Cisco.com account email address (*not* your Cisco.com user ID) and click **Login**.

Step 4 To log out, click on your user initials in the top-right corner, then click **Sign Out**.

If you're inactive for too long, you are automatically logged out and must log in again.

Main Window Controls

The main navigation controls in the Crosswork Cloud window are described below.



The following table describes the callouts that are shown above in the Crosswork Cloud home page.

Note The icons that appear depend on the Crosswork Cloud products for which you have a subscription.

Table 1: Crosswork Cloud Home Page Navigation Descriptions

Callout No.	Description
1	Click this icon to access Crosswork Cloud Network Insights features.
2	Click this icon to access Crosswork Cloud Traffic Analysis features. See About Traffic Analysis, on page 3 for more information.
3	Click this icon to access Crosswork Cloud Trust Insights features. See About Trust Insights, on page 5 for more information.
4	Activity Log. See View a List of Actions Performed, on page 241 for more information.
5	Help and Support. See Get Product Help and Support, on page 243 for more information.

Callout No.	Description
6	Click Settings to perform these tasks: • Manage Users, on page 233 • Import and Export Configuration Files, on page 239 • Purchase Crosswork Cloud • View Your Subscription and Licenses
7	The menu items that appear in this column depend on the product icon you select. This column typically contains the features organized into the following categories: • Monitor • Tools • Configure
8	Click your user initials to view the following options: • **View in Fullscreen**—Allows Crosswork Cloud to expand in fullscreen mode. • **My settings**—Allows you to view your role and provider. You can also change your timezone and change the user interface theme. See Modify User Settings, on page 281 for more information. • **My API Keys**—Allows you to generate a new API key or view existing API keys. See Crosswork Cloud APIs, on page 245 for more information. • The organization to which your username belongs. If you belong to more than one organization, you can switch between organizations by selecting the checkbox next to the organization to which you want to switch. • **Sign Out**—Logs you out of Crosswork Cloud.

Set Your Home Page

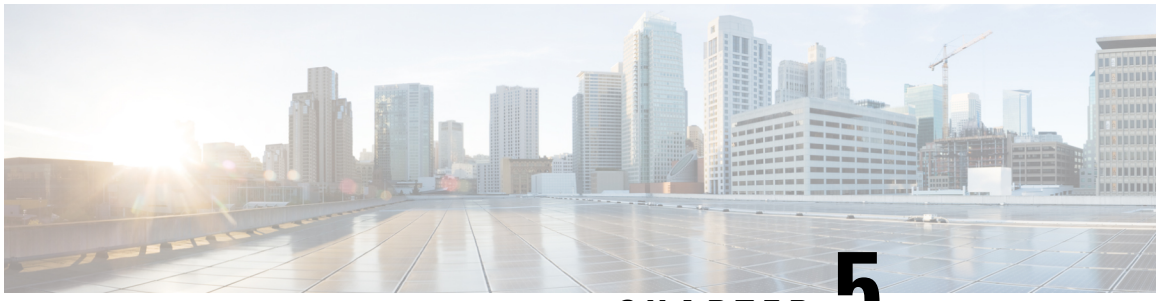
You can set a specific Cisco Crosswork Cloud page to be your default home page. When you specify a home page, that page is displayed after you log in to Cisco Crosswork Cloud.

Step 1 Log in to Cisco Crosswork Cloud. See Log In, on page 11 for more information.

Step 2 In the navigation pane on the left side of the Cisco Crosswork Cloud window, hover your cursor over the menu item for which you want to make your home page.

Step 3 Click the pin icon that appears.

When you log out and then log back in, the page you pinned appears.



CHAPTER 5

Use Setup Tools

Use External Routing Express Setup

Note This feature is for Crosswork Network Insights only.

To help set up your environment and ready to use, you can use the Express Setup feature.

You cannot use Express Setup to modify any previously added ASN.

Step 1 From the main window, click **Express Setup** at the bottom left of the page. You can also access the Express Setup tool by clicking **Help & Support**, then clicking **Express Setup**.

Step 2 Follow the prompts and enter the required information.

If you enter an ASN that was previously added, you receive an error message indicating any existing associated prefixes or policies. You must first delete and unlink any existing policies as explained in the error message.

Step 3 When the Express Setup finishes successfully, Crosswork Cloud Network Insights displays the changes based on the information you provided:

- The policies to create. You can view the autogenerated policy name, the policy type (ASN or Prefix), and the rules contained in that policy.
- The ASNs to subscribe (if you specified an ASN policy).
- The prefixes to subscribe (if you specified a prefix policy).
- The endpoints to link (if specified). You can view the endpoint name, type, and the policies associated to the endpoint.

Step 4 Review the changes, then click **Submit** to save the changes.

When the thresholds specified in the rules contained in the policy are crossed, Crosswork Cloud Network Insights generates an alarm and sends the alarm notification to the endpoint associated to the policy.

Use the Traffic Analysis Setup Checklist

Note This feature is for Crosswork Traffic Analysis only.

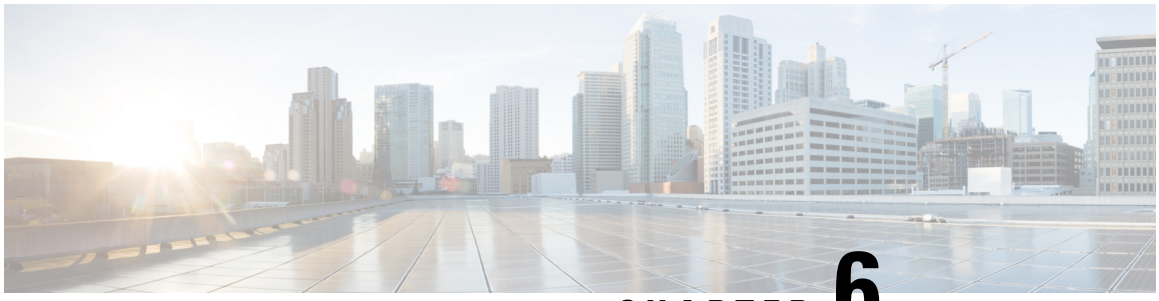
To help set up your environment and ready to use, you can use the Crosswork Cloud Traffic Analysis Setup Checklist feature.

Step 1 From the main window, click **Setup Checklist** at the bottom left of the page. You can also access the Setup Checklist tool by clicking **Help & Support**, then clicking **Setup Checklist**.

Step 2 Verify that each step in the checklist includes a green checkmark.

Step 3 Click the blue modify link next to any step that does not have a green checkmark.

This takes you to the corresponding page in which you can make edits to correct the errors.



CHAPTER 6

Install Crosswork Data Gateway

Install Crosswork Data Gateway

Crosswork Data Gateway is required for Crosswork Cloud Traffic Analysis and Crosswork Cloud Trust Insights only. It is not required for Crosswork Cloud Network Insights.

Prior to Crosswork Data Gateway installation, review the steps outlined in one of the following topics:

- Workflow: Add a Crosswork Data Gateway to Crosswork Cloud Trust Insights , on page 175
- Workflow: Add a Crosswork Data Gateway to Crosswork Cloud Traffic Analysis , on page 173

Note For Crosswork Data Gateway 6.0.1 and later, you have the option to create an enrollment token within Crosswork Cloud and then install a Crosswork Data Gateway. For earlier Crosswork Data Gateway versions, you must install a Crosswork Data Gateway first and manually enter the Data Gateway information in Crosswork Cloud.

Install a Crosswork Data Gateway as explained in the Cisco Crosswork Data Gateway Installation and Configuration Guide for Cloud Applications.

Add Crosswork Data Gateway Information

As part of the Data Gateway deployment process, an enrollment token (a unique registration file) must be created to enroll the Crosswork Data Gateway into Crosswork Cloud.

Starting with Crosswork Data Gateway 6.0.1, an enrollment token can be created in the Crosswork Cloud UI and then embedded during VM installation. The .json registration file contains unique digital certificates that are used to enroll the Crosswork Data Gateway into Crosswork Cloud. This method automatically enrolls a Crosswork Data Gateway in Crosswork Cloud and is less prone to potential problems than the older method.

For Crosswork Data Gateway versions earlier that 6.0.1, you must first Install Crosswork Data Gateway, generate an enrollment token from the Crosswork Data Gateway interactive console, and then manually enter Crosswork Data Gateway information in Crosswork Cloud.

Note

- While the procedure documented here describes the steps to use the newer method (if you are using Crosswork Data Gateway 6.0.1 or later), you have the option to use the older method (see Manually Add Crosswork Data Gateway Information, on page 180).
- If you use a firewall on your Data Gateway egress traffic, ensure that your firewall configuration allows cdg.crosswork.cisco.com and crosswork.cisco.com.

Step 1 From the main window, navigate to or > **Configure** > **Data Gateways** and then click **Add Data Gateway**.

Step 2 Choose to do one of the following:

- For Crosswork Data Gateway 6.0.1 and later, continue to Step 3.
- For earlier Crosswork Data Gateway versions, click **Registration File** and go to Manually Add Crosswork Data Gateway Information, on page 180.
- If you need to download the latest supported Crosswork Data Gateway version, click **Download CDG Image**.

Step 3 Click **Use Enrollment Token**.

Step 4 You can create a new token or use an existing one. Do one of the following:

- **Create a new token**
  - **a.** Click **Create Enrollment Token**.
  - **b.** Enter the following:
    - **Token Name**: Specify a unique name to the token that you are creating.
    - **Description**: Enter a detailed description of the token.
    - **Number of Uses**: Specify the permissible number of token uses. The maximum token usage limit is 50.
    - **Valid Until**: Specify the validity period for the token. The maximum duration is 366.
  - **c.** Click **Create**.
- **Use an existing token**
  - **a.** Select the row corresponding to the token that you intend to use.

    When selecting an existing token, consider its expiration date. If the Data Gateway will not be installed and registered prior to the expiration date, Cisco recommends you avoid using that token.

    You can review the **Valid Until** column on the **Add Crosswork Data Gateway** page to determine the expiration information.
  - **b.** Click **View Enrollment Token**.
    - **Token Name**: Specify a unique name to the token that you are creating.

- **Description**: Enter a detailed description of the token.
- **Number of Uses**: Specify the permissible number of token uses. The maximum token usage limit is 50.
- **Valid Until**: Specify the validity period for the token. The maximum duration is 366.

c. Click **Create**.

Step 5 Click **Copy** to copy the token. Paste the content in a local file. During Crosswork Data Gateway installation, you will need to paste the enrollment token in the following platforms:

- VMware
  - vCenter vSphere Client—Paste the token text into the **Auto Enrollment Package Transfer > Enrollment Token UI** field
  - OVF Tool—Locate the script and under the `## Enrollment Token for Crosswork Cloud` section, paste the token text after `CloudEnrollmentToken=`
- OpenStack—Locate the config.txt file and under the `## Enrollment Token for Crosswork Cloud` section, paste the token text after `CloudEnrollmentToken=`
- Amazon EC2—Paste the token in the CloudFormation template or as part of the user data after `CloudEnrollmentToken=`

Step 6 Install Crosswork Data Gateway.

Step 7 After Crosswork Data Gateway is installed, navigate back to > **Data Gateways** > **Use Enrollment Token**.

Step 8 Click **Next**. The newly installed Crosswork Data Gateway should appear with the Enrollment State as **Pending**.

Step 9 Click **Allow** to authorize the Crosswork Data Gateway access.

Step 10 Click **Next** after reviewing the Device information.

Step 11 Click **Accept** after reviewing the Network information.

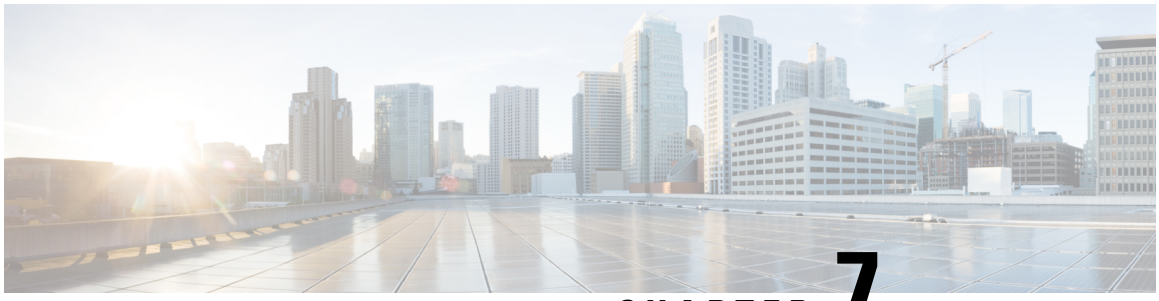
Step 12 After a few minutes, verify that your Crosswork Data Gateway is successfully connected. Click **Data Gateways**, click on the name of the Crosswork Data Gateway, and verify the following values for the Crosswork Data Gateway you added:

- **Connectivity**: Session Up
- **Admin State**: Enabled
- **Container Image**: Matched

You may need to refresh the page to see the changes.

PART III

Monitor Your Network



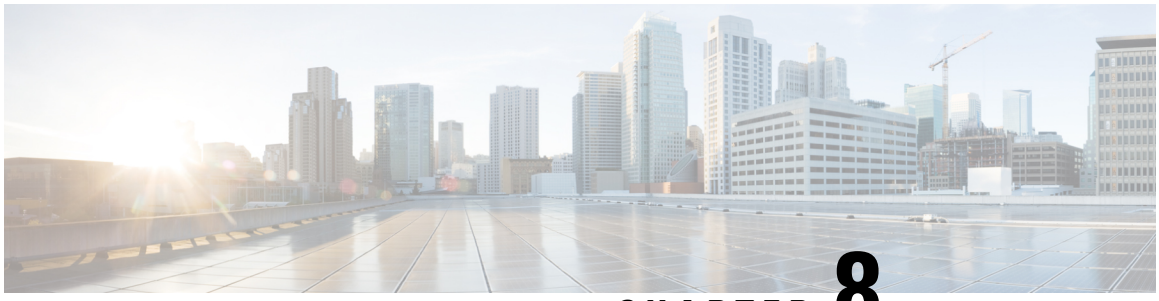
CHAPTER 7

Monitor Overview

Monitoring Overview

Each Crosswork Cloud product displays different information when you select **Monitor** > **Overview**, but all the Overview monitoring give you an overall look at the health of your system.

From the **Time Range** drop-down list, select a value to display overview information during a specific time period.



CHAPTER 8

Monitor Alarms

To help you quickly troubleshoot problems, you can easily view policy violations in the Alarms page (**Monitor** > **Alarms**). The Alarms page allows you to view active alarms, acknowledged alarms, or alarm history.

Alarm Descriptions

This section contains a list of alarms and linked descriptions. Alarms are triggered when a rule is violated in a policy.

Table 2: Crosswork Cloud Network Insights Alarms

Unexpected AS Prefix, on page 289	Prefix Withdrawal, on page 301	Upstream AS Change, on page 313
AS Origin Violation, on page 291	ROA Expiry, on page 303	Valid AS Path Violation, on page 315
New AS Path Edge, on page 293	ROA Failure, on page 305	Peer Down, on page 317
AS Path Length Violation, on page 295	ROA Not Found, on page 307	Advertised Prefix Count, on page 319
Parent Aggregate Change, on page 297	DNS Root Prefix Withdrawal, on page 309	Prohibited IP Prefix, on page 321
Prefix Advertisement, on page 299	Subprefix Advertisement, on page 311	

Table 3: Crosswork Cloud Traffic Analysis Alarms

Gateway Connectivity, on page 323	Device Connectivity, on page 325	Interface TX Utilization, on page 327

Interface RX Utilization, on page 329	Prefix Utilization, on page 331	

Table 4: Crosswork Cloud Trust Insights Alarms

Gateway Connectivity, on page 323	Device Running Configuration Change, on page 337	Hardware Integrity Validation
Device Connectivity, on page 325	Device SSH Host Key Violation	Mismatched Files
Device Certificate Expiring, on page 333	Dossier Collection Failure, on page 341	Package Validation
Device Certificate Violation	Expired Device Certificate, on page 343	Unknown Files

View All Alarms

Active alarms are generated when any condition in your policies are met.

To view descriptions of the possible alarms on the Alarms page, see Alarm Descriptions, on page 25.

Step 1 In the main window, click **Monitor** > **Alarms**.

Step 2 Click one of the following tabs at the top of the **Alarms** page:

- **Active**—Displays a list of all active alarms, which are sorted by priority.
- **Acknowledged**—Displays a list of all acknowledged alarms, which are sorted by priority.
- **History**—Displays historic alarms for which you can specify a time range from the **Timeframe** drop-down list. For more information, see View Alarm History, on page 27.

Step 3 You can sort columns in ascending or descending order. Hover your cursor in any column heading, then click the downward arrow that appears to change the sort order or to enter text on which to filter.

Step 4 To put the alarm in Acknowledged state, click the box next to an alarm, then click **Acknowledge**.

Step 5 To temporarily suspend alerts for an alarm, click the box next to an alarm, then click **Snooze**.

a) Select the time range for which you want to snooze the alarm, then click **Snooze**. Crosswork Cloud will not send notifications for this alarm for the time period you select.

View Alarm Details

You can view detailed information about a specific alarm.

Step 1 From the main menu, click **Monitor** > **Alarms**.

Step 2 Click the specific alarm for which you want to see details. The Alarm Details page appears.

Step 3 Using the buttons located on the top-right corner, you can perform one of the following operations associated with this alarm:

- For Network Insights, click **Remove Prefix/ASN from Policy** to remove the prefix or ASN and the rule that triggered the alarm from the policy. For Traffic Analysis or Trust Insights, click **Edit Policy** to make any changes to the policy.
- Click **Snooze** to temporarily suspend alerts for the alarm, select the time range for which you want to snooze the alarm, then click **Snooze**. Crosswork Cloud will not send notifications for this alarm for the time period you select.

  After you snooze an alarm, the alarm moves from the **Active** alarm page to the **Acknowledged** alarm page. From **Alarms** > **History** tab, you will see that the alarm state is set to **Snoozed** and shows how long it will remain in that state. To cancel a snoozed alarm, go back to the Alarm details page and click **Unacknowledge**.
- Click **Acknowledge** to put the alarm in Acknowledged state, meaning it is recognized and acknowledged.

  After you acknowledge an alarm, the alarm moves from the **Active** alarm page to the **Acknowledged** alarm page.

Step 4 Click on one of the tabs to view additional information about the alarm.

View Alarm History

The Alarm history page displays historic alarms for which you can specify a time range. By default, alarms are sorted by the most recent **Event At** date. The history of an alarm includes every state transition that occurred during its lifecycle. Alarm history records are never altered.

Step 1 From the main menu, click **Monitor > Alarms**.

Step 2 From the **Timeframe** drop-down list, select a time period that you are interested in. The window updates, displaying alert information for the time range you selected.

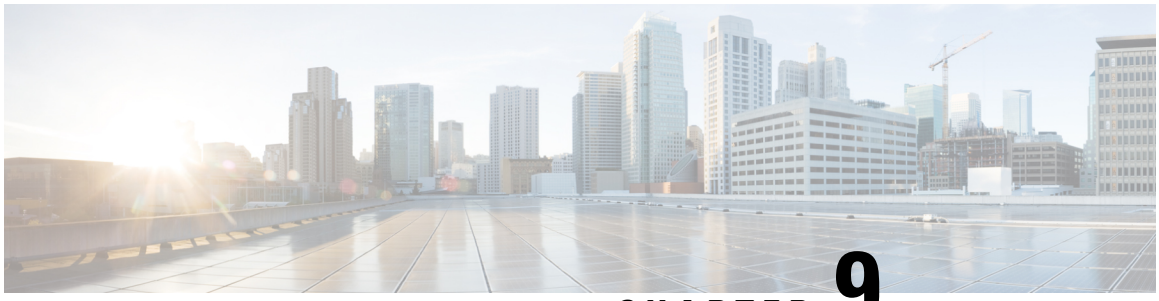
Step 3 You can filter any columns that display the **Add Filter** text. Click **Add Filter** and enter text on which you want to filter.

Step 4 Under the **Timeframe** drop-down list, click  to do any of the following tasks:

- **Customize Columns**—By default, not all available columns are displayed. Select this option to add, remove, or reorder columns.
- **Export CSV**—Select this option to export all currently loaded rows.

  Note Loaded rows are rows that are currently visible and may only be a subset of the total. You can scroll down to load more rows.

- **Save Table Settings**—Select this option to save any customized table settings. This includes any column width resizing, the addition or removal of columns, and any applied filters. After you initially save a table setting, you can later choose to **Remove Table Settings** or **Update Table Settings**.



CHAPTER 9

Monitor ASNs

View All ASNs

You can view all ASNs as described in the following steps:

Step 1 In the main window, click **External Routing Analytics > Monitor > ASNs**.

Crosswork Cloud Network Insights displays information in the following columns:

- ASN—The ASN.
- Policy—The policy associated with the ASN.
- Tags—List of tags associated with the ASN.
- Active Alarms—Number of active alarms associated with the ASN.
- Severity—The highest alarm level (High, Medium, or Low) associated with the ASN.
- Last Active Alarm—The alarm type, day, and time of the last active alarm associated with the ASN.

Step 2 To view more details about a specific prefix, click the ASN. See View ASN Details, on page 30.

Step 3 To add a new ASN, click **Monitor ASNs**. For more information, see Add an ASN to Monitor, on page 67.

View ASN Details

Step 1 In the main window, click **External Routing Analytics > Monitor > ASNs**.

Step 2 To view more details about a specific ASN, click the ASN name.

Step 3 Click one of the following tabs to display more details about the ASN:

- **Overview**—Contains summary information about your ASN. See ASN Overview Details, on page 30 for more details.
- **Alarms**—Provides details about alarms associated with the ASN. See ASN Alarm Details, on page 31 for more details.
- **Traffic**—Provides details about any traffic running on the ASN.
- **BGP Updates**—Contains details about the BGP updates, as reported by peers, that triggered alarms. See ASN BGP Update Details, on page 32 for more details.
- **Looking Glass**—Contains looking glass information for the ASN. See ASN Looking Glass Details, on page 32 for more details.
- **ROA**—Contains details about all known ROAs associated with the ASN. See ASN ROA Details, on page 33 for more details.
- **RPSL**—Contains RPSL data that is associated with the ASN. See ASN RPSL Coverage, on page 34 for more details.
- **Reports**—Lists the reports available for this ASN. To set up a report, click **Configure**. For more information, see Configure ASN Routing Reports, on page 195.

ASN Overview Details

To view ASN overview details, in the main window, click **External Routing Analytics > Monitor > ASNs**, click the name of the ASN, and then click the **Overview** tab.

Crosswork Cloud Network Insights displays ASN overview details as described in the following table.

Table 5: ASN Overview Details Field Descriptions

Field	Description
Linked Policy	The policy associated with the ASN.
Tags	User-specified tags that are applied to the ASN.
Last Active Alarm	List of last active alarms associated with the ASN.
Originating Prefixes	The number of orginating prefixes for the ASN.

Field	Description
Summary	Summary data including a map showing the geographical location and number of peers.
IRR/RPSL data	Provides the RPSL information for the ASN. Crosswork Cloud Network Insights displays the RPSL databases in which it found information for the ASN. Crosswork Cloud Network Insights retrieves the list of observed prefixes originating from the ASN, compares this with the information in the RPSL records, and determines if the origin ASNs match. The **Valid RPSL Prefix Coverage** indicates the number of prefixes in which Crosswork Cloud Network Insights validated that the prefix originates from the same ASN as specified in the RPSL database. Click on the number to view more RPSL details. See ASN RPSL Coverage, on page 34 for more information.
Peers	Number of peers and a map indicating the location of the peers. Click **Table** for a tabular view of peers.
Notes	Any user-configured notes associated with the ASN.

ASN Alarm Details

To view ASN alarm details, in the main window, click **External Routing Analytics > Monitor > ASNs**, click the name of the ASN, and then click the **Alarms** tab.

Crosswork Cloud Network Insights displays ASN alarm details as described in the following table.

Table 6: ASN Alarm Details Field Descriptions

Field	Description
Alarm state	Click any of the following alarm states: • **Active**—Crosswork Cloud Network Insights displays a list of all active alarms, which are sorted by priority. • **Acknowledged**—Crosswork Cloud Network Insights displays a list of all acknowledged alarms, which are sorted by priority.
Alarm Details	Details about the alarm.
# Peers	The number of peers that reported the violation.
Severity	The configured severity level of the alarm.
Activated	Date and time the alarm occurred.
Notes	Any user-entered notes about the alarm.

ASN BGP Update Details

To view ASN BGP update details, in the main window, click **External Routing Analytics > Monitor > ASNs**, click the name of the ASN, and then click the **BGP Updates** tab.

Crosswork Cloud Network Insights displays ASN BGP update details as described in the following table.

Table 7: ASN BGP Update Details Field Descriptions

Field	Description
Timeframe	Specify a timeframe by selecting a value from the **Timeframe** drop-down list.
Peer AS	The Peer AS from which the BGP update was received.
Prefix	The prefix IP address from which the BGP update was received.
AS Path	The AS routing path.
Communities	The communities path attribute, if applicable.
Update Type	The BGP update type.
Last Updated	Date and time of the last BGP update.

ASN Looking Glass Details

To view ASN looking glass details, in the main window, click **External Routing Analytics > Monitor > ASNs**, click the name of the ASN, then click the **Looking Glass** tab.

Crosswork Cloud Network Insights displays ASN looking glass details as described in the following table.

Table 8: ASN Looking Glass Field Descriptions

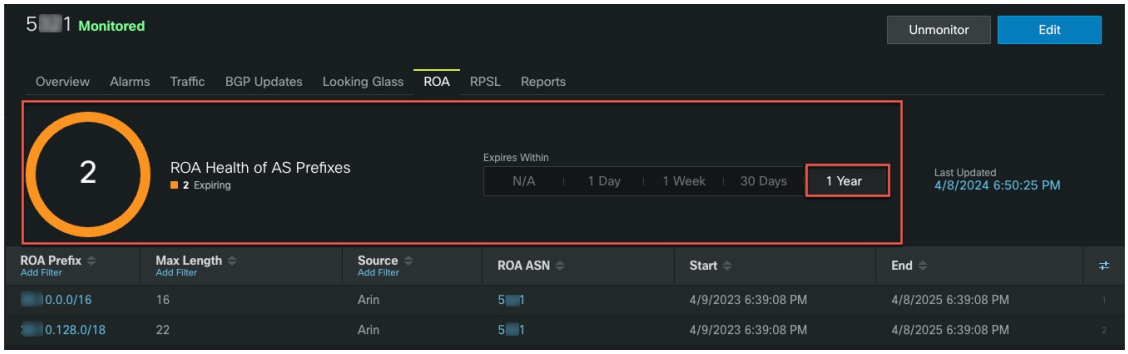
Field	Description
Prefix	The prefix IP address from which the BGP update was received.
Reporting Peers	The number of reporting peers.
Valid	Indicates whether the prefix is valid.
Subscribed	Indicates whether you are subscribed to the specific prefix.
Valid RPSL	Indicates if Crosswork Cloud Network Insights validated that the prefix originates from the same ASN as specified in the RPSL database.

ASN ROA Details

The ASN Route Origin Authorization (ROA) page (**External Routing Analytics > Monitor > ASNs > *asn-id* > ROA** tab) lists the ASN prefixes with active and expiring ROAs. To filter which prefixes are active or expiring within a given time range, select an option under the **Expires Within** field.

The following example shows two ROA prefixes that will expire within a year. You can find the details for the ROA prefixes listed in the table.

Figure 1: ASN ROA Page



Note There may be cases where a prefix is displayed with an expired ROA certificate. In these cases, the end date will be noted in red text. This can happen between updates where the certificate was valid at the time of the last update, but is now expired. The prefix entry will be removed in the next update.

Table 9: ASN ROA Descriptions

Column/Field	Description
Last Updated	The last date and time that information was retrieved
ROA Prefix	The prefix that the ROA authorizes the ASN to advertise. The ROA can cover a range of subnets for the base prefix as determined by Max Length. The total number of prefixes for the ASN that have an ROA with each status.
Max Length	The maximum prefix length of the most specific IP prefix that the ROA authorizes the ASN to advertise.

Column/Field	Description
Source	The organization that published the ROA. Examples: • American Registry for Internet Numbers (ARIN) • Internet Numbers Registry for Africa (AFRINIC) • Asia-Pacific Network Information Centre (APNIC) • Latin American and Caribbean Internet Addresses Registry (LACNIC) • Réseaux IP Européens (RIPE NCC)
ROA ASN	The AS number that is authorized by the ROA to originate the prefix.
Start	The start date and time for which this ROA is considered valid.
End	The end date and time for which this ROA is considered expired.

ASN RPSL Coverage

To view ASN RPSL details, in the main window, click **External Routing Analytics > Monitor > ASNs**, click the name of the ASN, then click the **RPSL** tab.

Crosswork Cloud Network Insights gathers the RPSL records for all the prefixes it observes originating from the ASN and displays the RPSL records as described in the table below. Crosswork Cloud Network Insights determines if the BGP prefix updates for an ASN matches the RPSL ASN record associated with that prefix.

Note There could be more than one row in the table for a particular prefix. This is because Crosswork Cloud Network Insights displays all records for a given prefix. If there are two RPSL records in a database, and each specifies a different origin ASN for the prefix, Crosswork Cloud Network Insights displays both records.

Table 10: ASN RPSL Details Field Descriptions

Field	Description
View options	Select which RPSL records you want to view: • All—Display all RPSL records. • Valid—Display valid and partial-match RPSL records in which Crosswork Cloud Network Insights validated that the prefix originates from the same ASN as specified in the RPSL database. • Mismatch—Display RPSL records in which the prefix originated from a different ASN than specified in the RPSL database. • No RPSL—Display prefixes that have no RPSL records.

Field	Description
Last Scan	The date and time Crosswork Cloud Network Insights last scanned the RPSL databases. Crosswork Cloud Network Insights scans RPSL databases once per day. To view the specific date and time Crosswork Cloud Network Insights scanned each RPSL database, click on the date. This helps you determine when Crosswork Cloud Network Insights last retrieved data from the RPSL databases.
Prefix	The prefix originating from this ASN, as observed by Crosswork Cloud Network Insights.
Source	The RPSL database source from which Crosswork Cloud Network Insights retrieved this record. Because prefixes can have records in multiple RPSL databases, Crosswork Cloud Network Insights displays each database source in a new row.
Origin ASN	The ASN that is specified in the *origin* attribute in the RPSL record.
Description	The *descr* attribute in the RPSL route/route6 record, which typically contains a description about the route record.
Member Of	The *member-of* attribute in the RPSL route/route6 record, which indicates the route-set with which the route/route6 record is associated.
Classification	Crosswork Cloud Network Insights determines if the BGP prefix updates for an ASN matches the RPSL ASN record associated with that prefix. When Crosswork Cloud Network Insights cannot find an RPSL record for an exact match of the prefix, it examines its parent's RPSL record to determine the classification. The classification values can be: • Mismatch—Indicates that Crosswork Cloud Network Insights has determined that the prefix has an origin ASN different from that specified in the RPSL database. • Exact Match—Indicates that Crosswork Cloud Network Insights validated that the prefix originates from the origin ASN specified in the RPSL record for that prefix. • Partial Match—Indicates that Crosswork Cloud Network Insights validated that the prefix originates from the ASN specified as the origin ASN in the RPSL record of the *parent* for that prefix (while not an exact prefix match, an RPSL record for the supernet was present). • No RPSL—Indicates that Crosswork Cloud Network Insights did not find any RPSL records for the prefix or its parent in any RPSL databases.
Last Updated	The date and time of the latest *changed* attribute in the RPSL record for the prefix or its parent.

View ASN Traffic Details

Note This feature is for Crosswork Traffic Analysis only.

You can view traffic details for one or multiple ASNs.

Step 1 In the main window, click **Traffic Analysis > Monitor > ASNs**.

Crosswork Cloud Traffic Analysis displays the traffic information for all ASNs.

Step 2 To view traffic details for a specific ASN, click on the ASN name or number in the first column.

Step 3 To compare traffic details for two or more ASNs, click the check box next to the ASNs, then click **Traffic Comparison** at the top of the table.

Crosswork Cloud Traffic Analysis displays traffic information for all selected ASNs.

View Daily ASN Changes (ASN Routing Report)

Each ASN Routing Report instance summarizes and identifies the *differences* in AS peerings (new, changed, inactive) and originated prefixes (new, changed, deleted) since the last time a report for the ASN was generated. This daily report can help you focus on potential problems or gaps in RIR/RPSL/ROA configuration that need to be addressed for the ASN and its associated prefixes. Each report instance is sent to the endpoint(s) you configured and contains direct links to the Crosswork Cloud Reports UI. This procedure describes how to navigate through the UI to see the contents of a report instance.

Before you begin

You must have an ASN Routing Report configured before viewing the daily reports. For more information, see Configure ASN Routing Reports, on page 195.

Step 1 In the main window, click **External Routing Analytics > Monitor > ASNs**.

Step 2 Click the name of the ASN and then then click **Reports**.
All reports that have been generated for this ASN are listed with high level details on this page.

Step 3 Click on a report instance name.
By default, the Summary page displays a high level count of AS peering and prefix changes.

Step 4 Click one of the following **AS Peering Changes** values:

- **New**—The AS Peers page displays any new AS peerings since the last report instance.
- **Changed**—The AS Peers page displays a list of AS peerings that have changed since the last report instance.
- **Inactive**—The AS Peers page displays any AS peerings that have been marked inactive since the last report instance. An AS peering is marked inactive if there have been no prefix notifications that contain this ASN peering (ASN does not appear in any AS paths) with the selected ASN for at least 30 days. The **Last Seen** column displays the last time the AS peer was active.

Note For more information, see AS Peers Report, on page 37.

Step 5 Click any **IPv4/IPv6 Prefix Changes** values:

- **New**—The IPv4/IPv6 Prefix page displays any new prefixes observed originating from this ASN since the last report instance.
- **Changed**—The IPv4/IPv6 Prefix page a list of prefixes observed originating from this ASN and have changed since the last report instance.
- **Deleted**—The IPv4/IPv6 Prefix page displays a list of prefixes that have been withdrawn since the last report instance.

Note For more information, see IPv4 and IPv6 Prefix Report, on page 38.

AS Peers Report

The AS Peers page displays the ASNs that the selected ASN is peering with, along with details that have changed since the last generated report instance.

Note By default, the page only shows AS peerings with New, Active Changed, or Inactive states. To view all AS peerings and states, include Active in the filter, or reset the filter to view the complete set of AS peerings that also includes the Active (but unchanged) AS Peerings.

- **Peer ASN**—The ASN peering with the ASN of interest.
- **Peering Type**—The peering type indicates whether the peer ASN is immediately upstream or downstream of the ASN of interest.
- **Peering State**—Displays the ASN Peering state at the time the report instance was generated. The following list shows the possible states for the ASN Peering:
  - **Active:** The peering between the two ASNs has been observed. This is either the first report instance generated or nothing has changed about this peering since the last report instance.
  - **Active Changed:** The peering has been active, but has changed since the last report instance.
  - **New:** This is a new ASN peering. This peering was not in the previous report instance.
  - **Inactive:** An inactive state means that the peering between the two ASNs has not appeared in any AS paths for at least 30 days.
- **Prefix Count**—Indicates the number of prefixes whose advertisements contain the AS peering in the AS path.
- **New Prefix Count**—Indicates the number of new prefixes being advertised.
- **First Seen/Last Seen**—Displays the first or last time the ASN peering appeared in the AS path of a prefix notification.

IPv4 and IPv6 Prefix Report

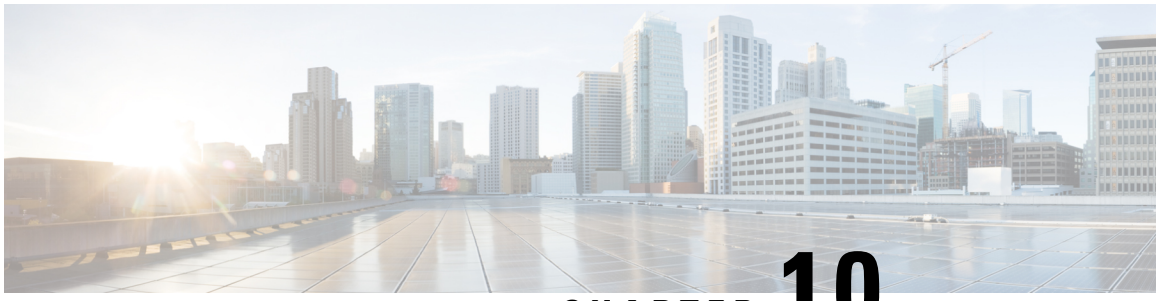
The IPv4 and IPv6 Prefix pages displays the prefix status and details at the time the report instance was generated.

Note By default, the page only shows prefixes with New, Active Changed, or Inactive states. To view all AS peerings and states, include **Active** in the filter, or reset the filter to view the complete set of prefixes that also includes the Active (but unchanged) prefixes.

The following details are displayed:

- **Prefix**—Lists all the prefixes of the selected ASN.
- **Subscribed**—Displays the subscription status at the time the report was generated.
- **RIR Information**—Displays the Whois information if it is available for IPv4 prefixes. This column currently does not apply to IPv6 prefixes.
- **Health**—An IPv4 prefix **Needs Attention** if either the RIR information or ROA records are unavailable or not associated with it. An IPv6 prefix **Needs Attention** if there are no ROE records associated with it.
- **Prefix State**—Displays the prefix status at the time the report instance was generated. When the prefix has been active, but has changed since the day before, the state is **Active Changed**.
  - **Active:** The prefix has been observed originating from the ASN. This is either the first report instance generated or nothing has changed about this prefix since the last report instance.
  - **Active Changed:** The prefix has been active, but has changed since the last report instance.
  - **New:** This is a new ASN prefix. This prefix was not in the previous report instance.
  - **Deleted:** The prefix has been withdrawn since the last report instance.
- **RPSL Status**—Displays the RPSL information at the time the report instance was generated. If the RPSL information has been found and the origin ASN matches the ASN it is observed to be originating from, the RPSL status is **Valid**. If an RPSL record is found, but the origin ASN in the record does not match the origin ASN observed, the RPSL status is **Mismatch**. If there are no RPSL records associated with the prefix, the status is **Not Found**.
- **ROA Status**—**Expiring Soon** indicates that ROA records associated with the prefix will expire within a day. You may want to filter the column with the **Expiring Soon** status so that you can update the record if necessary. View the ROA Expiring ROA Count column to see the number of records associated with the selected status.
- **RIR State**—Displays the state of the RIR information for the prefix at the time the report instance was generated. If the RIR information has been found and the origin ASN matches the ASN it is observed to be originating from, the RIR status is **Valid**. If RIR information is found, but the origin ASN in the record does not match the origin ASN observed, RIR status is **Mismatch**. If RIR information is not found for the prefix, the status is **Not Found**.
- **Valid RPSL** —Indicates the number of valid RPSL records for the prefix.
- **Expiring ROA** —Indicates the number of ROA records that are expiring for that prefix within a day.

- **Peer Count** —Indicates the number of peers that are advertising that prefix.



CHAPTER 10

Monitor Prefixes

Prefixes Overview

When you start with Crosswork Cloud Network Insights, you begin by adding prefixes. After you add prefixes, the prefixes window provides a consolidated view of prefixes, associated policies, and other useful information for monitoring large networks. The **External Routing Analytics > Monitor > Prefixes** window:

- Provides a location for storing and tracking your prefix information.
- Displays prefix state, alarm status, and prefix details.
- Monitors prefixes from worldwide vantage points, detecting regional events that might otherwise be overlooked by a single vantage point monitoring system.
- Lets you subscribe or unsubscribe from prefixes.

Add Prefixes

Step 1 In the main window, click **Prefixes**.

Step 2 Click **Subscribe to Prefixes**.

Step 3 Click on one of the following tabs:

- **Manual**—Enter the prefix IP addresses to which you want to subscribe. To add multiple prefixes, enter a comma (,) between each one. You can't add prefix masks smaller than /8. For example, you can't add a prefix such as 1.1.0.0/3.
- **ASN Lookup**—Enter an ASN for which you want to search for associated prefixes.
- **CSV Overwrite**—Upload a CSV file that contains prefix information. See Upload a Configuration File, on page 239 for more information.

Step 4 If you selected **Manual** or **ASN Lookup**, after you enter the required information, click **Next**.

Step 5 If you previously created a policy, select a policy to associate to the prefix from the **Policy** drop-down list. See Add Crosswork Cloud Network Insights Policies, on page 77 for more information.

Note You can associate a prefix to *one* policy only.

Step 6 (Optional) Enter meaningful text in the Tags field.

Note If you have entered more than one prefix, the policy and tag you specify is applied to all prefixes.

Step 7 Review your changes, then click **Submit** to apply your changes.

View All Prefixes

You can view all prefixes as described in the following steps:

Step 1 In the main window, click **External Routing Analytics > Monitor > Prefixes**.

Crosswork Cloud Network Insights displays a list of prefixes with information in the following columns:

- Prefix—The prefix IP address.
- Policy—The policy associated with the prefix.
- Tags—List of tags associated with the prefix.
- Active Alarms—Number of active alarms associated with the prefix.
- Severity—The alarm level (High, Medium, or Low) associated with the prefix.
- Last Active Alarm—The alarm type, day, and time of the last active alarm associated with the prefix.

Step 2 To view more details about a specific prefix, click the IP address of the prefix. See View Prefix Details, on page 42.

Step 3 To add a new prefix, click **Subscribe to Prefixes**. See Add Prefixes, on page 63.

View Prefix Details

You can view detailed information about a specific prefix.

Step 1 In the main window, click **External Routing Analytics > Monitor > Prefixes**.

Step 2 To view more details about a specific prefix, click the IP address of the prefix.

Step 3 Click one of the following tabs to display more details about the prefix:

- **Overview**—Contains summary information about your prefix. See Prefix Overview Details, on page 43 for more details.

- **Alarms**—Provides details about alarms that are associated with the prefix. See Prefix Alarm Details, on page 44 for more details.
- **BGP Updates**—Contains details about the BGP updates, as reported by peers, that triggered alarms. See Prefix BGP Update Details, on page 44 for more details.
- **Looking Glass**—Contains looking glass information for the prefix. See Prefix Looking Glass Details, on page 45 for more details.
- **ROA**—Contains details about all known ROAs associated with the prefix. See Prefix ROA Details, on page 45 for more details.
- **RPSL**—Contains Routing Policy Specification Language (RPSL) data that is associated with the prefix. See Prefix RPSL Details, on page 46 for more details.

Prefix Overview Details

To view prefix overview details, in the main window, click **External Routing Analytics > Monitor > Prefixes**, click the IP address of the prefix, then click the **Overview** tab.

Crosswork Cloud Network Insights displays prefix overview details as described in the following table.

Table 11: Prefix Overview Details Field Descriptions

Field	Description
Linked Policy	The policy associated with the prefix.
Last Modified	Date and time the prefix was most recently modified.
Tags	User-specified tags that are applied to the prefix.
Last Active Alarm	List of last active alarms associated with the prefix.
Summary	Summary data including a map showing the geographical location and number of peers. The estimated prefix geolocation is based on the geolocation of a sampling of IPs in the prefix that matches the address information from the Registrar. The location confidence level is calculated as one of the following: **Low**, **Med**, or **High**.
Valid RPSL coverage	The total number of RPSL records for this prefix that have an origin ASN matching the ASN observed by Crosswork Cloud Network Insights. See Prefix RPSL Details, on page 46 for more information.
Peers	Number of peers and a map indicating the location of the peers. Click **Table** for a tabular view of peers.
Contacts	Contact information for the prefix.
Origins	Origins details including observed values and from where they are derived.

Field	Description
Observed	Observed values and from where they are derived.
Upstream	Upstream details and from where they are derived.
Notes	Any user-entered notes associated with the prefix.

Prefix Alarm Details

To view prefix alarm details, in the main window, click **External Routing Analytics > Monitor > Prefixes**, click the IP address of the prefix, then click the **Alarms** tab.

Crosswork Cloud Network Insights displays prefix alarm details as described in the following table.

Table 12: Prefix Alarm Details Field Descriptions

Field	Description
Alarm state	Click any of the following alarm states: • **Active**—Crosswork Cloud Network Insights displays a list of all active alarms that are sorted by priority. • **Acknowledged**—Crosswork Cloud Network Insights displays a list of all acknowledged alarms that are sorted by priority.
Alarm Details	Details about the alarm.
# Peers	The number of peers that reported the violation.
Severity	The configured severity level of the alarm.
Activated	Date and time the alarm occurred.
Notes	Any notes entered about the alarm.

Prefix BGP Update Details

To view prefix BGP update details, in the main window, click **External Routing Analytics > Monitor > Prefixes**, click the IP address of the prefix, then click the **BGP Updates** tab.

Crosswork Cloud Network Insights displays prefix BGP update details as described in the following table.

Table 13: Prefix BGP Update Field Descriptions

Field	Description
Timeframe	Specify a specific timeframe by selecting a value from the **Timeframe** drop-down list.
Peer AS	The Peer AS from which the BGP update was received.

Field	Description
Prefix	The prefix
AS Path	The AS routing path.
Communities	The communities path attribute, if applicable.
Update Type	The BGP update type.
Last Updated	Date and time of the last BGP update.

Prefix Looking Glass Details

To view prefix looking glass details, in the main window, click **External Routing Analytics > Monitor > Prefixes**, click the IP address of the prefix, then click the **Looking Glass** tab.

Crosswork Cloud Network Insights displays looking glass details as described in the following table.

Table 14: Prefix Looking Glass Field Descriptions

Field	Description
Peer AS	The Peer AS.
Peer	The peer identifier, which is used to identify the peer but keep its identity private.
AS Path	The AS routing path.
Communities	The communities path attribute, if applicable.
Last Modified	Date and time the prefix was most recently modified.

Prefix ROA Details

To view prefix ROA details, in the main window, click **External Routing Analytics > Monitor > Prefixes**, click the IP address of the prefix, then click the **ROA** tab.

The Prefix Route Origin Authorization (ROA) page (**External Routing Analytics > Monitor > ASNs > *prefix-ip-address* > ROA** tab) lists the ASN prefixes with active and expiring ROAs. To filter which prefixes are active or expiring within a given time range, select an option under the **Expires Within** field.

Crosswork Cloud Network Insights displays prefix ROA details as described in the following table.

Table 15: Prefix ROA Details Field Descriptions

Column/Field	Description
Last Updated	The last date and time that information was retrieved
ROA Prefix	The prefix that the ROA authorizes the ASN to advertise.

Column/Field	Description
Max Length	The maximum prefix length of the most specific IP prefix that the ROA authorizes the ASN to advertise.
Source	The organization that published the ROA. Examples: • American Registry for Internet Numbers (ARIN) • Internet Numbers Registry for Africa (AFRINIC) • Asia-Pacific Network Information Centre (APNIC) • Latin American and Caribbean Internet Addresses Registry (LACNIC) • Réseaux IP Européens (RIPE NCC)
ROA ASN	The AS number that is authorized by the ROA to originate the prefix.
Start	The start date and time for which this ROA is considered valid.
End	The end date and time for which this ROA is considered expired.

Prefix RPSL Details

To view prefix RPSL details, in the main window, click **External Routing Analytics > Monitor > Prefixes**, click the IP address of the prefix, then click the **RPSL** tab.

Crosswork Cloud Network Insights compares the ASN record associated with the prefix in the RPSL database with the ASN record in the Whois database. Crosswork Cloud Network Insights displays the prefix RPSL details as described in the following table

Table 16: Prefix RPSL Details Field Descriptions

Field	Description
Last Scan	The date and time Crosswork Cloud Network Insights last scanned the RPSL databases. **External Routing Analytics > Monitor > Prefixes** scans RPSL databases once per day. To view the specific date and time Crosswork Cloud Network Insights scanned each RPSL database, click on the date. This helps you determine when Crosswork Cloud Network Insights last retrieved data from the RPSL databases.
Source	The RPSL database source from which Crosswork Cloud Network Insights retrieved this record. Because prefixes can have records in multiple RPSL databases, Crosswork Cloud Network Insights displays each database source in a new row.
Origin ASN	The prefix origin ASN that is specified in the RPSL record.

Field	Description
Description	The *descr* attribute in the RPSL route/route6 record, which typically contains a description about the route record.
Member Of	The *member-of* attribute in the RPSL route/route6 record, which indicates the route-sets with which the route/route6 record is associated.
Classification	Crosswork Cloud Network Insights compares the ASN record associated with the prefix in the RPSL database with the ASN record in the Whois database. When Crosswork Cloud Network Insights cannot find an RPSL record for an exact match of the prefix, it examines the RPSL record corresponding to its parent to determine the classification. The classification values can be: • Mismatch—Indicates that Crosswork Cloud Network Insights has determined that the prefix has an origin ASN different from that specified in the RPSL database. The **Overview** tab shows the observed ASN for this prefix, which does not match the origin ASN in the RPSL database. • Exact Match—Indicates that Crosswork Cloud Network Insights validated that the prefix originates from the origin ASN as specified in the RPSL record and the WhoIS database for that prefix. • Partial Match—Indicates that Crosswork Cloud Network Insights validated that the prefix originates from the ASN specified as the origin ASN in the RPSL record of the *parent* for that prefix (while not an exact match, an RPSL record for the supernet was present). • No RPSL—Indicates that Crosswork Cloud Network Insights did not find any RPSL records for the prefix or its parent in any RPSL databases.
Last Updated	The date and time of the latest *changed* attribute in the RPSL record for the prefix or its parent.

View Prefix Traffic Details

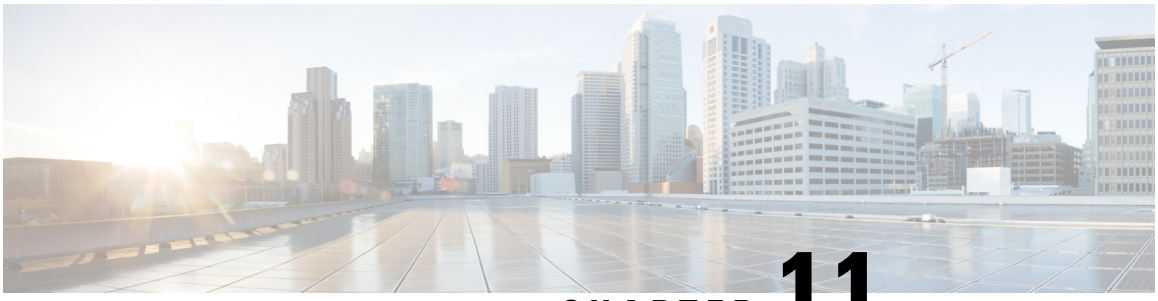
You can view traffic details for one or multiple prefixes.

Step 1 In the main window, click **Traffic Analysis > Monitor > Prefixes**.

Step 2 Filter and displays prefixes that are relevant to the device, device group, or tag group you select. You can also perform a search by entering specific prefix criteria. Select one of the following tabs:

- **Relevant Prefixes**—Select this tab to view a list of prefixes by device or device group.
- **Grouped by Tag**—Select this tab to view a list of prefixes by an assigned tag.
- **Search All**—Select this tab to enter additional prefix search criteria.

Step 3 To compare traffic details for two or more prefixes, click the check box next to the prefixes, then click **Traffic Comparison** at the top of the table.



CHAPTER 11

Monitor BGP Updates

View BGP Updates

Step 1 In the main window, click **External Routing Analytics > Monitor > BGP Updates**.

Step 2 From the **Timeframe** drop-down list, select a value to display changes during a specific time period.

The interactive dual-axis graph displays the BGP advertisements and withdrawals that occurred during that time range. The number of advertisements are represened on the left side of the graph. The number of withdrawals are represented on the right side of the graph.

Step 3 To further zoom into a specific time range (must be 10 or more minutes), click the starting point and drag to the end of the duration. Then, click **Zoom**. Notice that the table displays only the selected data.

Step 4 To filter data, click **Add Filter**.

Note In the AS Path column, numbers within circle icons denote a repeating AS. For example, the following example denotes two 20764 hops in the path:

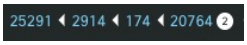
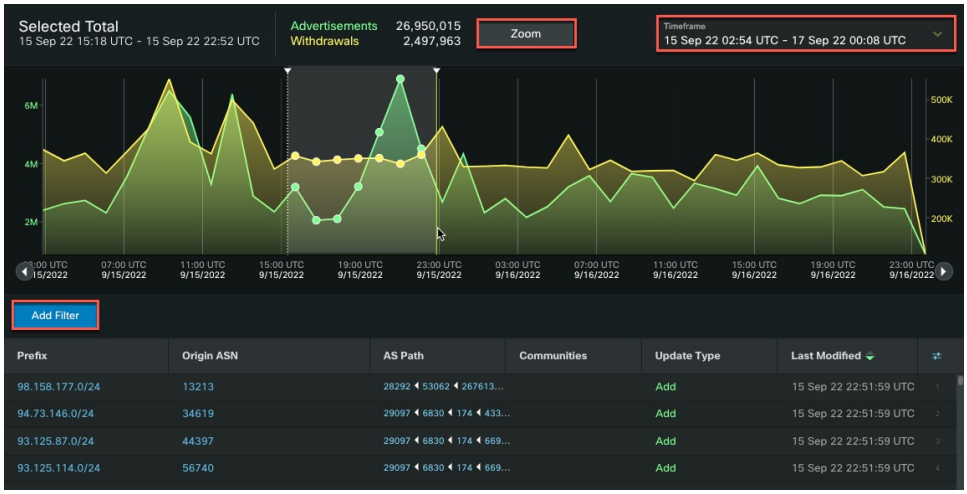
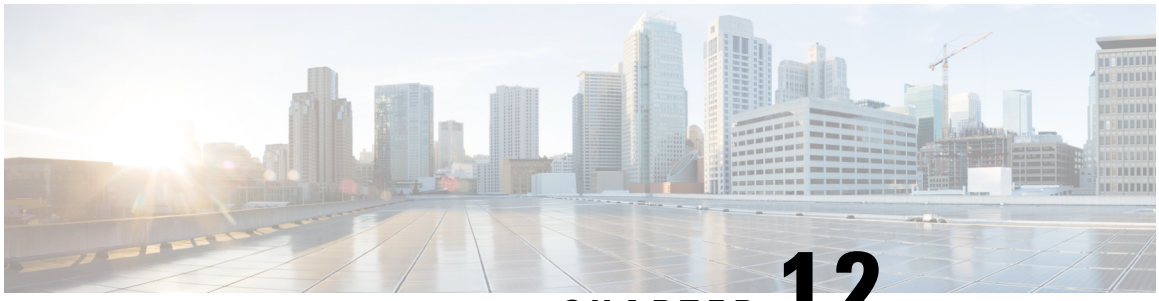


Figure 2: BGP Updates Page





CHAPTER 12

Monitor Devices

View Device Status

You can view device status to view connectivity and any errors.

Step 1 In the main window, click **Monitor** > **Devices**.

A list of previously added devices is displayed.

Step 2 Click on a device name in the **Device** column.

Detailed device information is displayed. By default, the **Status** tab is selected and displays overview information about the device. (Depending on the applications for which you have a license, separate product tabs also appear.)

Step 3 On the **Status** page, verify that there are no connectivity errors. Green arrows indicate working connectivity.

a. Verify the connection between Applications and Crosswork Data Gateway is working.

b. Verify the connection between Crosswork Data Gateway and the devices.

Step 4 Hover your cursor over any fields to display more details.

Step 5 To export a .json file containing device status, click **Export Status Report**.

View Device Traffic Details

You can view the receive (RX) and transmit (TX) traffic information for the devices that you added.

Note The data displayed in the graph may be delayed by five minutes since Netflow data is sent to the system every five minutes.

Step 1 In the main window, click **Traffic Analysis** > **Monitor** > **Devices**.

A list of previously added devices appears.

Step 2 Click the name of the device for which you want to see the details. By default, the Traffic Analysis tab is displayed.

Step 3 By default, the **Graphs** tab opens and displays RX and TX traffic metrics. From the Time drop-down list, select the timeframe for which you want to view the traffic information.

Step 4 After you make any changes, click the **Refresh** icon to update data.

Step 5 To view traffic details for the device interfaces, click the **Interfaces** tab.

Step 6 To view specific RX and TX data for an interface, click the interface name.

Step 7 To designate an interface as internal or external, check the check box next to one or more interfaces, then choose **Set External** or **Set Internal**.

The **Type** column updates to display the interface type.

View Trust Insights Details

You can view Crosswork Cloud Trust Insights details for devices you previously added.

Step 1 In the main window, click **Trust Insights** > **Monitor** > **Devices**.

A list of previously added devices appears.

Step 2 Click on the name of the device for which you want to see the details.

Step 3 By default, the **Trust Insights** tab opens. The rest of the device details page contains information organized into separate tabs. The following table describes the device detail information displayed under each tab.

Table 17: Trust Insights Device Detail Descriptions

Tab	Description
Platform	Displays information similar to the output of the *show platform* CLI command. To view more details, click the following tabs: • **Hardware**—Lists hardware node, type, state, HA state, and last seen information. Click on a name in the Node column to display specific information about that node. Crosswork Cloud Trust Insights displays a history of where this individual component was previously observed. The hardware component history tracks individual hardware FRUs, based on their confirmed serial number, across systems over time. • **Package Insights**—Lists packages on the device that are deactivated or have not been committed. The state can be one of the following: • **Active - Uncommitted**—The package is actively running on the device. If you want to save these changes, commit the package prior to rebooting the device. • **Deactivated**—The package is not actively running on the device. You can commit this change, otherwise the package will be active again after the device reboots or is activated manually. • **Packages**—Lists all the software packages. For more information, see View Device Software Changes, on page 54. • **Mismatched Files**—Displays a list of mismatched files on this device. For more information, see View Device Package Mismatched Files, on page 56.
Inventory	Lists the device hardware details such as serial numbers, models, firmware, and other information.
Changes	Shows hardware and software changes made to the device. See View Device Changes, on page 54 for more information.

View Device Inventory

Crosswork Cloud Trust Insights can display details about your hardware inventory, which can be helpful if you are troubleshooting hardware issues.

Step 1 In the Crosswork Cloud Trust Insights main window, click **Trust Insights > Monitor > Devices**.

Crosswork Cloud Trust Insights displays a list of previously added devices. See Add Devices, on page 164 for more information.

Step 2 Click on the name of the device for which you want to see inventory details.

If **Connected** appears next to the device name, the Crosswork Data Gateway has successfully connected to the device.

Step 3 Click the **Inventory** tab.

Crosswork Cloud Trust Insights displays all the hardware associated with the device you selected.

View Device Changes

You can view the device changes to understand what and when hardware and software changes were made.

Step 1 In the main window, click **Trust Insights > Monitor > Devices**.

Crosswork Cloud Trust Insights displays a list of devices that were previously added. See Add Devices, on page 164 for more information.

Step 2 Click on the name of the device for which you want to view the changes.

Crosswork Cloud Trust Insights displays overview information about the device.

Step 3 Click the **Changes** tab.

Trust Insights highlights observed events over a historical timeline for the device you selected.

Step 4 Click on a time frame for which you want to see the device changes.

Step 5 Click **Hardware** to view the hardware change details for the timeframe you selected.

Step 6 Click **Software** to view the software change details for the timeframe you selected.

Step 7 Click **Changes Only** to display only values that changed from the start to the end of the time period you selected.

View Device Software Changes

Crosswork Cloud Trust Insights provides a way to understand what software changes were made on your devices. You can view specific software changes made to your devices and observe where there are software mismatches between Known Good Values (KGVs) and what your device is currently running.

Step 1 In the main window, click **Trust Insights > Monitor > Devices**.

Crosswork Cloud Trust Insights displays a list of devices that were previously added. To add devices, see Add Devices, on page 164 for more information.

Step 2 Click on the name of the device for which you want to view the changes.

Step 3 By default, the **Trust Insights** tab opens.

Step 4 Under the **Platform** tab, click **Packages**, which appears under the graph.

Crosswork Cloud Trust Insights lists all the software packages.

In the **Package Integrity** column, Crosswork Cloud Trust Insights displays one of the following values:

- Changes detected—Indicates the correct software package was installed, but changes were made after the installation.
- Mismatch—Indicates the installed software package does not match the Known Good Value (KGV).
- Mismatch and changes detected—Indicates the installed software package does not match the KGV and changes were made after the installation.
- OK—The installed software package matches the KGV.
- Not supported—Fingerprinting is not enabled on the device or the software package fingerprint is missing in the dossier. If the latter is applicable and available for the device, you need to install an SMU that supports package integrity measurements.

  Note Cisco IOS XR Release 7.3.1 and later releases supports the fingerprint of packages. This feature helps in verifying the authenticity of an installable package using a Known Good Value (KGV) for each package. The installed and running software is compared with the KGV to determine whether the package is genuine.

- No KGV data—Crosswork Cloud Trust Insights is unable to compare the software package with KGVs because the package fingerprint is missing in the KGV. Crosswork Cloud Trust Insights does not recognize the package.

Step 5 Click on a link in the **Package Integrity** column to view additional details about the software files and packages on your device.

Crosswork Cloud Trust Insights displays the Software Integrity Analysis, which includes the following details:

- Package Signature Analysis—Displays details about any changes detected in the package signature. Crosswork Cloud Trust Insights evaluates the installed packages and displays measurements to indicate if the package signature is trustworthy. The following fields indicate package signature changes, and you can quickly validate if any of the hashes do not match:
  - Known Good Values Hash—Value designated by Cisco or previously designated in Crosswork Cloud Trust Insights.
  - Package Install Hash—Value at the time the package was installed.
  - Package Runtime Hash—Value of the package during runtime.
- File Signature Analysis—Displays details about the changes detected in the file signature. Each file that contains a mismatch is displayed along with the details about the mismatch. If a file does not have any mismatches, it does not appear in the list. You can view the hashes displayed in the columns to view where the mismatches occur. To quickly

view a list of mismatched files on this device click the **Mismatched Files** tab (see View Device Package Mismatched Files, on page 56).

View Device Package Mismatched Files

Crosswork Cloud Trust Insights allows you to quickly view a list of mismatched package files for a particular device. Mismatched files indicate software mismatches between Known Good Values (KGVs) and what your device is currently running.

Step 1 In the main window, click **Trust Insights > Monitor > Devices**.

Crosswork Cloud Trust Insights displays a list of devices that were previously added. To add devices, see Add Devices, on page 164 for more information.

Step 2 Click on the name of the device for which you want to view the mismatched files.

Step 3 By default, the **Trust Insights** tab opens.

Step 4 Under the **Platform** tab, click **Mismatched Files**, which appears under the graph.

Crosswork Cloud Trust Insights lists all the mismatched files found on that device.

In the **Mismatch Status** column, Crosswork Cloud Trust Insights displays one of the following values:

- **Runtime**—The KGV value does not match the value of the file during runtime.
- **OnDisk**—The KGV value does not match the hash of the file content currently on the disk.
- **OnDisk & Runtime**—The KGV value does not match the value of the file during runtime and the value at the time the package was installed.
- **Unknown**—Crosswork Cloud Trust Insights cannot determine the KGV value.

Step 5 From the **Mismatch Status** column, click the status value.

a) Click the **History** tab to view the file details. You can view the hashes displayed in the columns to quickly view where the mismatch occurs.

b) Click the **Seen Elsewhere** tab to view a list of devices that also have this mismatched file.

View File Anomalies

Note Devices running the following Cisco IOS XR versions are supported:

- 7.4.1
- 7.4.2
- 7.5.2

To help monitor malicious activity or tampering of Cisco IOS XR devices, you can view a list of unknown files for a particular device. Generally, any files that are "not expected" or significantly deviate from typical IOS XR files are flagged as unknown files. For example:

- Files that do not match known KGV filenames.
- Files where the metadata has changed, yet the SHAsum remains the same.
- Files that have known hashes but the filename or path does not match the KGV.

Step 1 In the main window, click **Trust Insights** > **Monitor** > **Devices**.

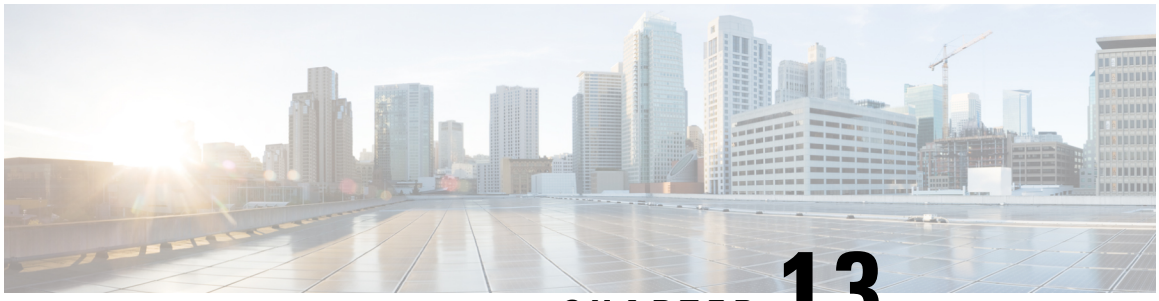
Crosswork Cloud Trust Insights displays a list of devices that were previously added. To add devices, see Add Devices, on page 164 for more information.

Step 2 Click on the name of the device for which you want to view unknown files.

Step 3 By default, the **Trust Insights** tab opens.

Step 4 Under the **Platform** tab, click **Unknown Files**, which appears under the graph.

Crosswork Cloud Trust Insights lists details of all the unknown files found on that device.



CHAPTER 13

Monitor Interfaces

View Interface Traffic Details

After you add devices, Crosswork Cloud Traffic Analysis gathers information about the interfaces. You can view traffic details about the interfaces.

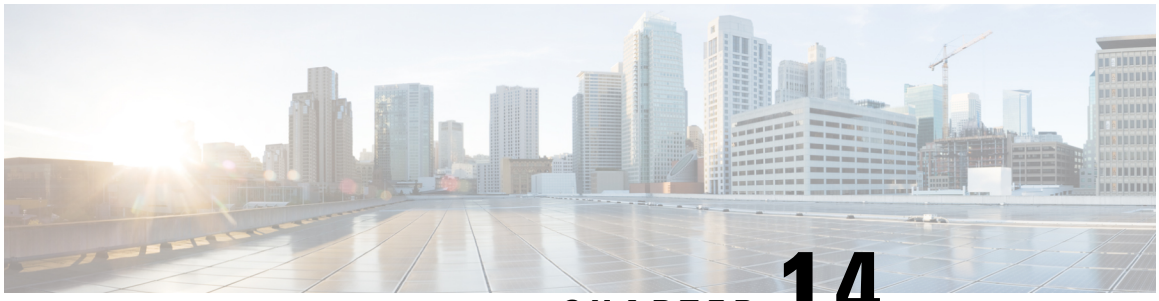
Step 1 In the main window, click **Traffic Analysis > Monitor > Interfaces**.

Step 2 Click on the interface name for which you want to see the traffic details.

Crosswork Cloud Traffic Analysis displays receive (RX) and transmit (TX) traffic information.

PART IV

Configure Crosswork Cloud



CHAPTER 14

Configure Prefixes

Add Prefixes

Step 1 In the main window, click **External Routing Analytics > Configure > Prefixes**.

Step 2 Click **Subscribe to Prefixes**.

Step 3 Click on one of the following tabs:

- **Manual**—Enter the prefix IP addresses to which you want to subscribe. To add multiple prefixes, enter a comma (,) between each one. You cannot add prefix masks smaller than /8. For example, you cannot add a prefix such as 1.1.0.0/3.
- **ASN Lookup**—Enter an ASN for which you want to search for associated prefixes.
- **CSV Overwrite**—Upload a CSV file that contains prefix information. See Upload a Configuration File, on page 239 for more information.

Step 4 If you selected **Manual** or **ASN Lookup**, after you enter the required information, click **Next**.

Step 5 If you previously created a policy, select a policy to associate to the prefix from the **Policy** drop-down list. See Add Crosswork Cloud Network Insights Policies, on page 77 for more information.

Note You can associate a prefix to *one* policy only.

Step 6 (Optional) Enter meaningful text in the Tags field.

Note If you have entered more than one prefix, Crosswork Cloud Network Insights applies the policy and tag you specify to all prefixes.

Step 7 Review your changes, then click **Submit** to apply your changes.

Edit and Unlink Prefixes

You can edit prefixes by adding or deleting tags that are associated with each prefix. You can also remove a prefix from a policy.

Step 1 In the main window, click **External Routing Analytics > Monitor > Prefixes**.

Step 2 Click the check box next to one or more prefixes you want to edit, then click **Edit**.

Note If you selected more than one prefix to edit, Crosswork Cloud Network Insights applies the changes to all selected prefixes.

Step 3 To apply your changes, click **Submit**.

Step 4 To remove a prefix from a policy, select the check box next to one or more prefixes, then click **Unlink**.

Step 5 Confirm that you want to unlink the prefix, then click **Unlink**.

Note When you unlink a prefix, the prefix stays in the list of prefixes in Crosswork Cloud Network Insights and can be edited, but can no longer be monitored. Alternatively, you can unsubscribe from a prefix, which removes the prefix from Crosswork Cloud Network Insights. See Delete and Unsubscribe Prefixes, on page 64 for more information.

Delete and Unsubscribe Prefixes

Before you delete prefixes, we recommend that you export and save your current configuration. See Download a Configuration File, on page 240.

You can unlink a prefix, which keeps the prefix in the list of prefixes, but doesn't allow you to monitor or edit the prefix. Alternatively, you can unsubscribe from a prefix, which removes the prefix. The following steps explain how to unsubscribe a prefix.

Step 1 In the main window, click **External Routing Analytics > Configuration > Prefixes**.

Step 2 Click the check box next to the prefix you want to delete, then click **Unsubscribe**.

Step 3 In the confirmation dialog box, click **Unsubscribe**.

Temporarily Suppress Prefix Notifications

The Pause Prefix feature temporarily suppresses prefix alarm notifications that are triggered by a linked policy violation. For example, you might not want to receive alarm notifications during a network maintenance operation. Rather than unsubscribing and then linking the prefix back to the policy later, you can “pause” a prefix for a set amount of time.

Note the following behavior when enabling the Pause Prefix feature:

- You can pause a subscribed prefix for up to 90 days.

- Crosswork Cloud Network Insights does not send Alarm notifications for a paused prefix when a violation occurs in an associated policy.
- Alarms do not appear in the **Active** alarms page. However, they continue to appear in the alarm **History** page.
- Crosswork Cloud Network Insights will send a cleared alarm notification if the following conditions are met:
  - The alarm was active before the prefix was paused.
  - The alarm was cleared while the prefix was paused.

Note Crosswork Cloud Network Insights will not send any further alarm notifications until the prefix resumes.

- After the prefix resumes:
  - Crosswork Cloud Network Insights will not send alarm notifications that were previously suppressed if they were cleared before the prefix resumes.
  - Crosswork Cloud Network Insights sends active alarm notifications that were previously suppressed if they are still in active state.

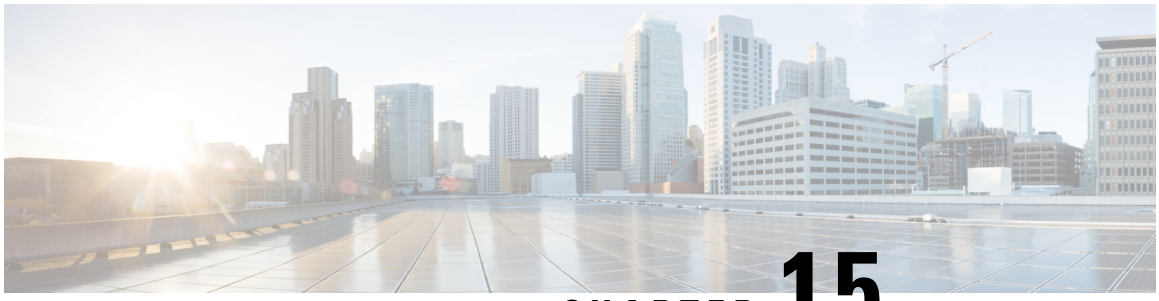
Step 1 In the main window, click **External Routing Analytics** > **Configure** > **Policies** > ***Policy-name*** and click the **Prefixes** tab.

Step 2 Click the check box next to one or more prefixes that you want to temporarily pause notifications for.

Step 3 Click **Pause Prefix**.

Step 4 From the **Pause Duration** drop-down list, choose the time range (1 week, 1 month, 2 months, or 3 months) for which you want to stop alarm notifications for this prefix.

Step 5 Click **Pause**. The prefix status displays **Paused** and when the prefix will resume. To cancel a paused prefix, check the check box next to the prefix and click **Resume Prefix**.



CHAPTER 15

Configure ASNs

Add an ASN to Monitor

Step 1 In the main window, click **External Routing Analytics > Configure > ASNs**.

Step 2 Click the **Monitor ASNs** button.

Step 3 In the **ASNs** field, enter the ASN. To add multiple ASNs, enter a comma (,) between each one.

Step 4 Click **Next**.

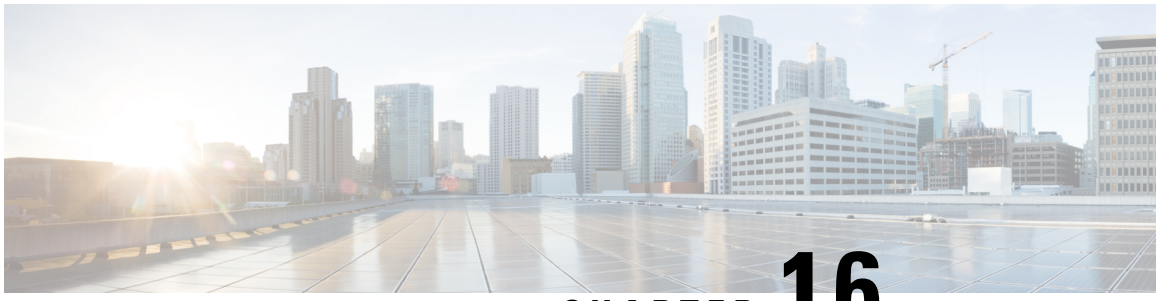
Step 5 If you previously created a policy, select a policy to associate to the ASN from the **Policy** drop-down list. See Configure Policies, on page 77 for more information.

Note You can associate an ASN to *one* policy only.

Step 6 (Optional) Enter meaningful text in the **Tags** field.

Note If you have entered more than one ASN, Crosswork Cloud Network Insights applies the policy and tag you specify to all ASNs.

Step 7 Review your changes and then click **Save** to apply the changes.



CHAPTER 16

Configure Peers

Import Peers

If your organization has existing peer configurations in BGPmon that are enabled, you can import the peers from BGPmon.

Step 1 In the main window, click **External Routing Analytics > Configure > Peers**.

Step 2 Click **Peermon Import**.

Step 3 Enter the email address associated with each peer in the Peermon table, then click **Request**.

Crosswork Cloud Network Insights sends a confirmation email to the address you entered.

Step 4 Click the approval link in the email to import your peer configurations from BGPmon into Crosswork Cloud Network Insights.

If the email confirmation link expired before you clicked on it, you can resend the confirmation email by clicking **Restart Import**.

After you click the approval link, Crosswork Cloud Network Insights transfers the peers from BGPmon and displays a message after successfully importing the peer information. The imported peers appear under the **Peers** menu.

Add Peers

This is the first step when adding a peer to Crosswork Cloud.

Step 1 In the main window, click **External Routing Analytics > Configure > Peers**.

Step 2 Click **Add Peer**.

Step 3 Complete the fields described in the following table:

Field	Description
IP	IP address of the peer.
Name	Unique name of the peer. The peer name should not match any of your other peers.
ASN	ASN to which the peer belongs.
City	City in which the peer is located.
Country	Country in which the peer is located.
Contact Email	Contact email address for the peer.
Description	Description of the peer.
Policy	Select a policy to associate to the peer.
Tags	(Optional) Enter meaningful text to apply to the peer.

Step 4 Click **Save**.

Step 5 Obtain the Cisco route server and ASN details. For more information, see View Peer Details, on page 70.

Step 6 Configure the peer device. For more information, see Configure Peer Devices, on page 72.

View Peer Details

You can view detailed information about a specific peer. You can also obtain the Cisco route server and ASN information that is needed to configure the peer device (see Configure Peer Devices, on page 72).

Step 1 In the main window, click **External Routing Analytics > Configure > Peers**.

Step 2 To view more details about a specific peer, click the IP address of the peer. Crosswork Cloud Network Insights displays more details about the peer as described in the following tables.

Note From this page, you can also Edit Peers, Disable Peers, or Remove Peers this peer by clicking on the corresponding button.

Table 18: Overview

Field	Description
Linked Policy	The policy associated with the prefix.

Field	Description
Stats Updated	Time when the statistics was last updated.
Sessions Established/Dropped	The number of times the BGP session between the route server peer and your peer was Established/Dropped.
Last Reset	Time when the session was last reset.
Last Reset Reason	The reason the BGP session was reset.
Last Active Alarm	Last active alarm associated with the peer. Click the alarm to view more details. To view a list of last active alarms, click **View All**.
This Peer	Displays information about the peer.
BGP Session	Displays information about the current BGP session.
Route Server and ASN	Information about the route server peer router with which your peer has a BGP session that is established or is trying to establish. This information is needed to configure a peer device. For more information, see Configure Peer Devices, on page 72.
Number of Prefixes	A 7-day timeline that displays the average number of prefixes that are accepted by your peer.

Table 19: Alarms

Field	Description
Alarm state	Click any of the following alarm states: • **Active**—Crosswork Cloud Network Insights displays a list of all active alarms that are sorted by priority. • **Acknowledged**—Crosswork Cloud Network Insights displays a list of all acknowledged alarms that are sorted by priority.
View	Click **View** to view details about the alarm.
Rule	The rule that was violated.
Severity	The configured severity level of the alarm.
Activated	Date and time the alarm occurred.

Table 20: BGP Updates

Field	Description
Timeframe	Specify a timeframe by selecting a value from the **Timeframe** drop-down list.

Field	Description
Advertisements/Withdrawals	The total number of advertisements and withdrawals observed during the timeframe.
Prefix	The prefix IP address from which the BGP update was received.
Origin ASN	ASN it is observed to be originating from.
AS Path	The AS routing path.
Communities	The communities path attribute, if applicable.
Update Type	The BGP update type.
Last Modified	Date and time of the last BGP update.

Configure Peer Devices

You can use the following templates to apply configurations on the peer device.

Cisco IOS XE

```
router bgp <asn>
 bgp router-id <router-id>
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor <route-server-ipv4> remote-as 65179
 neighbor <route-server-ipv4> description Cisco CrossWork Route Server IPv4
 neighbor <route-server-ipv4> ebgp-multihop 255
 neighbor <route-server-ipv4> update-source <src-interface>
 !
 neighbor <route-server-ipv6> remote-as 65179
 neighbor <route-server-ipv6> description Cisco CrossWork Route Server IPv6
 neighbor <route-server-ipv6> ebgp-multihop 255
 neighbor <route-server-ipv6> update-source <src-interface>
 !
 address-family ipv4
  neighbor 172.31.20.53 activate
  neighbor 172.31.20.53 send-community both
  neighbor 172.31.20.53 filter-list 2 in
  neighbor 172.31.20.53 filter-list 1 out
 exit-address-family
 !
 address-family ipv6
  neighbor 172.31.20.53 activate
  neighbor 172.31.20.53 send-community both
  neighbor 172.31.20.53 filter-list 2 in
  neighbor 172.31.20.53 filter-list 1 out
 exit-address-family
!
ip as-path access-list 1 permit .*
ip as-path access-list 2 deny .*
```

where

- <*asn*> is the BGP AS number in your network.
- <*router-id*> is the BPG router ID in your network.
- <*src-interface*> is the BGP source interface in your network.

The following IPv4/IPv6 information is generated after the peer is added using the UI. For more information, see Add Peers, on page 69 and View Peer Details, on page 70.

- <*route-server-ipv4*> is the IPv4 address for the Cisco Route Server.
- <*route-server-ipv6*> is the IPv6 address for the Cisco Route Server.

Cisco IOS XR

```
router bgp <asn>
 address-family ipv4 unicast
 !
 address-family ipv6 unicast
 !
 neighbor <route-server-ipv4>
 remote-as 65179
 bgp router-id <router-id>
 ebgp-multihop 255
 description Cisco CrossWork Route Server IPv4
 update-source <src-interface>
 address-family ipv4 unicast
 route-policy DROP in
 route-policy PASS out
 !
 !
 neighbor <route-server-ipv6>
 remote-as 65179
 ebgp-multihop 255
 description Cisco CrossWork Route Server IPv6
 update-source <src-interface>
 address-family ipv6 unicast
 route-policy DROP in
 route-policy PASS out
!
route-policy PASS
 pass
end-policy
!
route-policy DROP
 drop
end-policy
!
```

where

- <*asn*> is the BGP AS number in your network.
- <*router-id*> is the BPG router ID in your network.
- <*src-interface*> is the BGP source interface in your network.

The following IPv4/IPv6 information is generated after the peer is added using the UI. For more information, see Add Peers, on page 69 and View Peer Details, on page 70.

- <*route-server-ipv4*> is the IPv4 address for the Cisco Route Server.
- <*route-server-ipv6*> is the IPv6 address for the Cisco Route Server.

Edit Peers

You can edit peers that you previously added or imported.

Step 1 In the main window, click **External Routing Analytics** > **Configure** > **Peers**.

Step 2 To edit one peer, click the IP address of the peer, then click **Edit**.

When editing a single peer, you can modify the name, city, country, contact, description, policy, and tag of the peer.

Step 3 Modify any of the fields, then click **Save**.

Step 4 To modify and apply the same changes to a group of peers, click the check box next to each peer you want to edit, then click **Edit**.

When editing multiple peers, you can modify the policy and tags that are assigned to the peers and deactivate or activate all peers.

Step 5 Modify any of the fields, then click **Submit**.

Disable Peers

When you disable a peer, Crosswork Cloud Network Insights temporarily stops collecting information from the peer and terminates the BGP session between the Crosswork Cloud Network Insights route server and your peer router. Crosswork Cloud Network Insights keeps the peer configuration in its database but discards the peer statistics, which includes the BGP session status and the number of IPv4 and IPv6 prefixes.

You can enable the peer later to resume data collection.

Alternatively, you can *remove* a peer to delete it from Crosswork Cloud Network Insights. You cannot recover any of its data after removing the peer. See Remove Peers, on page 75.

Step 1 In the main window, click **External Routing Analytics** > **Configure** > **Peers**.

Step 2 Click the IP address of the peer you want to deactivate.

Step 3 Click **Disable**.

A message appears to indicate the peer is disabled.

You can enable a peer that has been disabled. When you enable the peer again, Crosswork Cloud Network Insights uses the stored peer configuration, and the BGP peering session resumes between your peer router and the Crosswork Cloud Network Insights route server. After enabling a peer, it can take up to 30 mins for the statistics to appear on the peer details page.

Step 4 To restart data collection for the peer, click **Enable**.

A message appears to indicate the peer is enabled and Crosswork Cloud Network Insights resumes collecting data for the peer.

Remove Peers

When you remove a peer, all the peer data is deleted from Crosswork Cloud Network Insights. Crosswork Cloud Network Insights deletes the BGP peer configuration from its route server, and the BGP session between Crosswork Cloud Network Insights and your peer router terminates.

All peer data that is associated with the peer is discarded and cannot be recovered. You cannot reactivate a peer that has been removed.

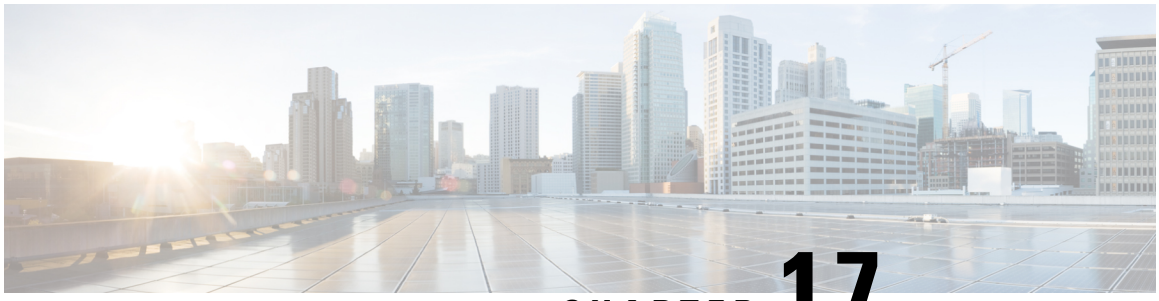
Alternatively, you can *disable* a peer, in which Crosswork Cloud Network Insights temporarily stops collecting information from the peer. See Disable Peers, on page 74.

Step 1 In the main window, click **External Routing Analytics > Configure > Peers**.

Step 2 Click the check box next to the peer you want to delete or click on the IP address, then click **Remove**.

Step 3 Confirm that you want to delete the peer by clicking **Remove**.

The peer and its previously collected data are deleted from Crosswork Cloud Network Insights.



CHAPTER 17

Configure Policies

Policies Overview

Policies and alarms can alert you to unexpected behavior which can help you identify possible misconfigurations, malicious routing activity, and network utilization issues. You use policies to monitor network operations (routing health, utilization, and so on). You create policies by defining a set of rules with specified threshold values. When a rule is violated and thresholds are exceeded, Crosswork Cloud activates an About Alarms that can be sent to a number of About Notification Endpoints.

In the main window, navigate to one of the following Crosswork Cloud applications to create, modify, or view policies:

- Crosswork Cloud Network Insights Policies, on page 77 (> **Configure** > **Policies**)— Monitors unexpected BGP advertisements.
- Crosswork Cloud Traffic Analysis Policies, on page 81 (> **Configure** > **Policies**)— Monitors relevant utilization abnormalities.
- Crosswork Cloud Trust Insights Policies, on page 83 (> **Configure** > **Policies**)— Monitors device integrity.

Crosswork Cloud Network Insights Policies

Add Crosswork Cloud Network Insights Policies

Note It is sometimes helpful to duplicate an existing policy and make minor modifications rather than creating a new policy. For more information, see Manage Crosswork Cloud Network Insights Policies, on page 79.

Step 1 In the main window, click > **Configure** > **Policies**.

Step 2 Click **Add Policy**.

Step 3 Click on one of the Crosswork Network Insights Alarm Types:

- **ASN Policy**
- **Prefix Policy**
- **Peer Policy**

Step 4 Enter a policy name in the **Name** field.

Step 5 To add a notification endpoint that receives notifications when a rule in the policy is violated, click **Add Endpoint**.

Step 6 If you selected to create a prefix policy, in the **Expected AS Path Editor** section, enter values for the following fields:

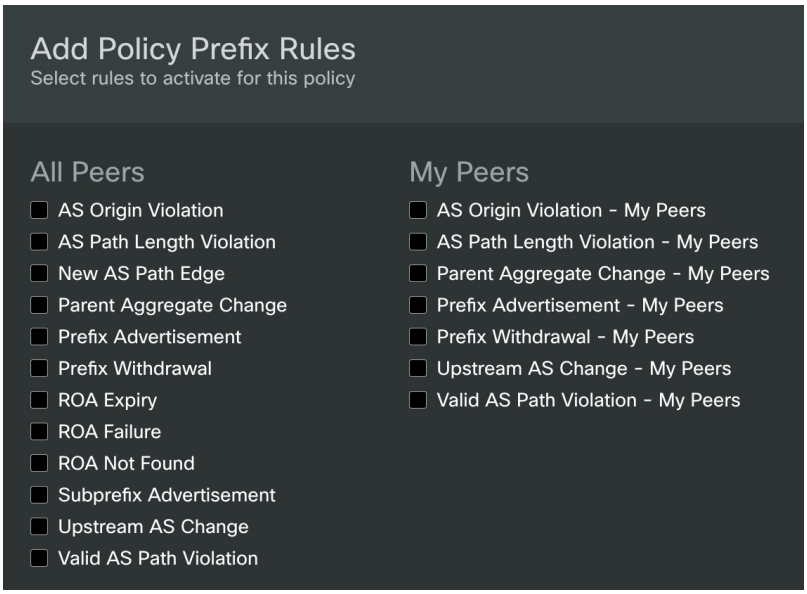
- **Origin ASNs**—The ASN origin, which is the route through which the prefix is advertised.
- **Upstream ASNs**—The ASN one hop before.
- Click **Configure** to enter a valid AS path pattern. Crosswork Cloud Network Insights compares the specified ASN pattern (the expected sequence of AS numbers in order) with the advertised AS path on a prefix and detects when they do not match.

Step 7 In the Rules section, click **Add Rule**, then select one or more rules to apply to the policy.

a) (*For Prefix policies only*) There are two **Prefix** policy rule categories available with certain View Subscription Plan Options: **All Peers** and **My Peers. My Peers** rules follow BGP updates *only* from your Add Peers, whereas **All Peers** follow BGP updates from your peers *and* global peers.

Check all rules which you would like to include in the Prefix policy and click **Save**.

Figure 3: Prefix Policy Rules: All Peers and My Peers



Step 8 For each rule, specify the following:

- Whether the rule is **Enabled** (default) or **Disabled**.
- **Peers to Resolve**—Enter the number of unique peers that should detect a specific event before silencing an alarm.
- **Peers to Trigger**—Enter the number of unique peers that should detect a specific event before triggering an alarm.
- **Severity**—Select the severity level of the alarm.

Step 9 In the Endpoints section, click **Add Endpoint**.

Step 10 Select an endpoint type from the **Endpoint Type** drop-down list.

Step 11 Click in the **Endpoint** field, then select an existing endpoint or click **Add Endpoint** and complete the required fields.

You can configure endpoints at any time. See Configure Notification Endpoints, on page 87 for more information.

Step 12 In the **Notes** field, enter any necessary notes.

Step 13 Click **Save**.

Manage Crosswork Cloud Network Insights Policies

To view, modify, or duplicate policies, do the following:

Step 1 In the main window, click  > **Configure** > **Policies**.

Step 2 Click the name of the policy for which you want to duplicate, manage, or view more details. Crosswork Cloud Network Insights displays additional details about the policy as described in the following table.

Table 21: Policy Details Field Descriptions

Tab	Field	Description
Overview The **Overview** tab contains details about the policy you specified.	Expected Origin ASNs	The ASN origin, which you specified when you created the policy, Crosswork Cloud Network Insights expects.
	Expected Upstream ASNs	The Upstream ASN that you specified when you created the policy.
	Valid AS Path Pattern	The Valid AS Path Pattern that you specified when you created the policy.
	Rules	List of rules in the policy. Crosswork Cloud Network Insights displays details about each rule, including the number of active alarms for each rule. To view the specific alarms for any rule, click **Active Alarms** in any of the rules.

Tab	Field	Description
Prefixes The **Prefixes** tab contains details about the prefixes associated with the policy.	Prefix	Lists the prefix IP address. Click on the IP address to view prefix details. See View Prefix Details, on page 42 for more information. Click **Link Prefixes** to link additional prefixes to the policy.
	Tags	Lists the tags associated with the prefix.
Alarms The **Alarms** tab contains details about alarms associated with the prefix.	Alarm state	Click any of the following alarm states: • **Active**—Crosswork Cloud Network Insights displays a list of all active alarms sorted by priority. • **Acknowledged**—Crosswork Cloud Network Insights displays a list of all acknowledged alarms sorted by priority. • **History**—Crosswork Cloud Network Insights displays a list of historic alarms for which you can specify a time range from the **Timeframe** drop-down list. To acknowledge or snooze an alarm, select the checkbox next to an alarm, then click **Acknowledge** or **Snooze**.
	Alarm Details	Details about the alarm.
	Trigger	The prefix or ASN that triggered the alarm.
	Rule	The rule that was violated.
	# Peers	The number of peers that reported the violation.
	Severity	The configured severity level of the alarm.
	Activated	Date and time the alarm occurred.
	Notes	Any user-entered notes.

Step 3 To modify the policy, click **Edit**.

a) Update notification endpoints, Origin and Upstream ASNs, AS path patterns, and rules as needed.

b) Click **Save**.

Step 4 To delete the policy, click **Remove**. Click **Remove** again to confirm removal.

Step 5 To copy an existing policy, click **Duplicate**.

a) By default, the name of the new policy begins with **Copy of** followed by the name of duplicated policy.

b) Make the necessary changes, then click **Save**.

Crosswork Cloud Traffic Analysis Policies

Add Crosswork Cloud Traffic Analysis Policies

Crosswork Cloud Traffic Analysis automatically creates two policies:

- Gateway Connectivity, on page 323—Monitors Crosswork Data Gateway connectivity to Crosswork Cloud.
- Device Connectivity, on page 325—Monitors device connectivity to the Crosswork Data Gateway.

To create additional policies that monitor TX, RX, and jumbo prefix utilization, do the following:

Note It is sometimes helpful to duplicate an existing policy and make minor modifications rather than creating a new policy. For more information, see Manage Crosswork Cloud Traffic Analysis Policies, on page 82.

Step 1 In the main window, click > **Configure** > **Policies**.

Step 2 Click **Add Policy**.

Step 3 Enter a policy name in the **Name** field.

Step 4 Under **Triggers**, click **Add Rules**.

Note If you choose to cancel during this procedure, the unfinished policy will still be listed in the Policies page.

Step 5 Check the Interface policies you want to create:

- **Interface TX Utilization**—Monitors transmitting traffic information. You specify the TX utilization range that will trigger an alarm.
- **Interface RX Utilization**—Monitors receiving traffic information. You specify the RX utilization range that will trigger an alarm.
- **Prefix Utilization**—Monitors jumbo prefix utilization. You specify the prefix utilization range that will trigger an alarm.

Step 6 For each rule, move the sliders to indicate utilization ranges and severity levels that will trigger alarms.

Step 7 Click **Next**.

Step 8 Under **Data**, click **Add** to select which interfaces you want to monitor.

Step 9 Follow the instructions displayed on the **Select Interfaces to Monitor** page, then click **Add**.

Step 10 Under **Actions**, click **Add Notification** until all the notification types you want sent (after a rule is triggered) is configured.

Step 11 Click **Save**.

Manage Crosswork Cloud Traffic Analysis Policies

To view, modify, or duplicate policies, do the following:

Step 1 In the main window, click > **Configure** > **Policies**.

Step 2 To modify the **Gateway Connectivity** or **Device Connectivity** policies, click **Details** in the respective window. For more information, see Gateway Connectivity, on page 323 and Device Connectivity, on page 325.

Step 3 To duplicate, manage, or view details of user created policies, click the name of the policy. Crosswork Cloud Traffic Analysis displays additional details about the policy as described in the following table.

Table 22: Policy Details Field Descriptions

Tab	Field	Description
Overview The **Overview** tab contains details about the policy you specified.	Triggers	Displays the interface rules configured for this policy.
	Data	Displays the monitored interfaces for this policy.
	Actions	Displays the endpoint notifications configured for this policy.
Alarms The **Alarms** tab contains details about alarms associated with the policy.	Alarm state tab	Click any of the following alarm states: • **Active**—Displays a list of all active alarms sorted by priority. • **Acknowledged**—Displays a list of all acknowledged alarms sorted by priority. • **History**—Displays a list of historic alarms for which you can specify a time range from the **Timeframe** drop-down list. To acknowledge or snooze an alarm, select the checkbox next to an alarm, then click **Acknowledge** or **Snooze**.

Step 4 To modify the policy, click **Edit**.

a) Update interface rules, monitored interfaces, and configured endpoint notifications as needed.

b) Click **Save**.

Step 5 To delete the policy, click **Remove**. Click **Remove** again to confirm removal.

Step 6 To copy an existing policy, click **Duplicate**.

a) By default, the name of the new policy begins with **Copy of** followed by the name of duplicated policy.

b) Click **Edit** to make the necessary changes, then click **Save**.

Crosswork Cloud Trust Insights Policies

Add Crosswork Cloud Trust Insights Policies

Crosswork Cloud Trust Insights automatically creates two policies:

- Gateway Connectivity, on page 323—Monitors Crosswork Data Gateway connectivity to Crosswork Cloud.
- Device Connectivity, on page 325—Monitors device connectivity to the Crosswork Data Gateway.

To create additional policies that monitor device integrity, do the following:

Note It is sometimes helpful to duplicate an existing policy and make minor modifications rather than creating a new policy. For more information, see Manage Crosswork Cloud Trust Insights Policies, on page 84.

Step 1 In the main window, click > **Configure** > **Policies**.

Step 2 Click **Add Policy**.

Step 3 Enter a policy name in the **Name** field and click **Next**.

Step 4 Under **Triggers**, click **Add Rules**.

Note If you choose to cancel during this procedure, the unfinished policy will still be listed in the Policies page.

Step 5 Check the Device rules you want to create:

- Device Certificate Expiring, on page 333
- Device Certificate Violation, on page 335
- Device SSH Host Key Violation, on page 339
- Device Running Configuration Change, on page 337
- Dossier Collection Failure, on page 341
- Expired Device Certificate, on page 343
- Hardware Integrity Validation, on page 345
- Mismatched Files, on page 347
- Package Validation, on page 349

- Unknown Files, on page 351

Step 6 For each rule, indicate severity level and attributes that will trigger an alarm.

Step 7 Click **Next**.

Step 8 Under **Data**, click **Add** to select which devices you want to monitor.

Step 9 Follow the instructions displayed on the **Select Devices** page, then click **Add**.

Step 10 Under **Actions**, click **Add Notification** until all the notification types you want sent (after a rule is triggered) is configured.

Step 11 Click **Save**.

Manage Crosswork Cloud Trust Insights Policies

To view, modify, or duplicate policies, do the following:

Step 1 In the main window, click > **Configure** > **Policies**.

Step 2 To modify the **Gateway Connectivity** or **Device Connectivity** policies, click **Details** in the respective window. For more information, see Gateway Connectivity, on page 323 and Device Connectivity, on page 325.

Step 3 To duplicate, manage, or view details of user created policies, click the name of the policy. Crosswork Cloud Trust Insights displays additional details about the policy as described in the following table.

Table 23: Policy Details Field Descriptions

Tab	Field	Description
Overview The **Overview** tab contains details about the policy you specified.	Triggers	Displays the device rules configured for this policy.
	Data	Displays the monitored devices for this policy.
	Actions	Displays the endpoint notifications configured for this policy.

Tab	Field	Description
Alarms The **Alarms** tab contains details about alarms associated with the policy.	Alarm state tab	Click any of the following alarm states: • **Active**—Displays a list of all active alarms sorted by priority. • **Acknowledged**—Displays a list of all acknowledged alarms sorted by priority. • **History**—Displays a list of historic alarms for which you can specify a time range from the **Timeframe** drop-down list. To acknowledge or snooze an alarm, select the checkbox next to an alarm, then click **Acknowledge** or **Snooze**.

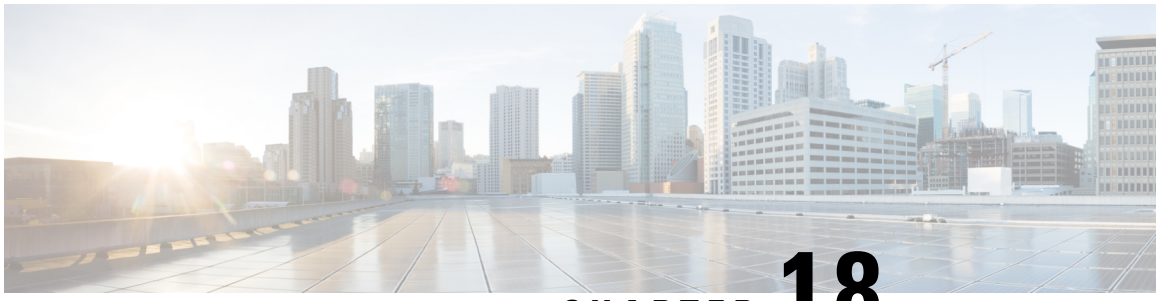
Step 4 To modify the policy, click **Edit**.

a) Update device rules, monitored devices, and configured endpoint notifications as needed.
b) Click **Save**.

Step 5 To delete the policy, click **Remove**. Click **Remove** again to confirm removal.

Step 6 To copy an existing policy, click **Duplicate**.

a) By default, the name of the new policy begins with **Copy of** followed by the name of duplicated policy.
b) Click **Edit** to make the necessary changes, then click **Save**.



CHAPTER 18

Configure Notification Endpoints

About Notification Endpoints

During policy creation, you can configure multiple endpoints to receive alarm notifications when a rule inside a policy is violated.

The following notification endpoint types are available:

- Email
- Google Storage
- Amazon S3
- SMS
- Slack
- WebEx
- Microsoft Teams
- PagerDuty

Endpoint Notification Content

Content and delivery of alarm notification information vary depending on the endpoint notification type. The types of information contained in the notification message are categorized as Raw Data or Summarized Data.

Raw Data

For Amazon S3 and Google Storage notification endpoints, the information is delivered in raw form as a series of JSON (JavaScript Object Notation) objects. A JSON object represents an alarm notification event as it appears in the system. These events are written into the configured S3 and Cloud Storage bucket as an object that corresponds to the current window of time (for example, the current minute). If there are no events

delivered during a given window, a JSON object is not written. For examples, see Amazon S3 and Google Storage Endpoint Notification Examples by Alarm Type, on page 94.

Summarized Data

The message contains a summary of events that occurred during a window of time. Typically, the message includes the total number of alarm transition events, specific alarm details from the first few events, and a link to view more events. The exact format and alarm details displayed depends on the endpoint type and corresponding constraints on message size (for example: SMS endpoints do not contain any specific alarm details since there is only enough room to display the total count).

Error Handling

If an endpoint fails to receive a notification, Crosswork Cloud attempts to deliver the notification until it succeeds or the notification no longer exists in the system. The latter case results in the notification endpoint not being delivered.

Configure Notification Endpoints

When a policy rule is violated, an alarm appears in the Alarms page. However, you may want Crosswork Cloud to also notify you or a group of users when an alarm occurs. You can configure an endpoint to receive alarm notifications.

You configure endpoint notifications within a policy or by clicking the Settings icon > **Global** > **Notifications**. Follow these steps to create an endpoint notification:

Step 1 In the main window, click > **Global** > **Notifications**.

Step 2 Choose the notification type for the endpoint you want to create:

- Email
- Configure Google Storage Endpoints
- Amazon S3
- Slack
- SMS
- Configure Webex Endpoints
- Configure Microsoft Team Endpoints
- PagerDuty

Note See also Notification Message Examples, on page 92.

Step 3 Click **Add *type* Endpoint**.

Step 4 Enter a name for the endpoint.

Step 5 Choose whether the endpoint is **Enabled** (default) or **Disabled**.

Step 6 Enter the required information for the endpoint type you chose in Step 2.

Step 7 (Optional) Enter any notes.

Step 8 Click **Save**.

Step 9 After you receive a confirmation code from Crosswork Cloud, enter the code in the **Verification Code** field, then click **Verify**.

If you select **Skip for Now**, Crosswork Cloud creates the endpoint but will not send any notifications to the endpoint until you verify the endpoint by entering the verification code.

Configure Google Storage Endpoints

You can configure Crosswork Cloud to send notification logs to Google Cloud Storage.

Before you begin

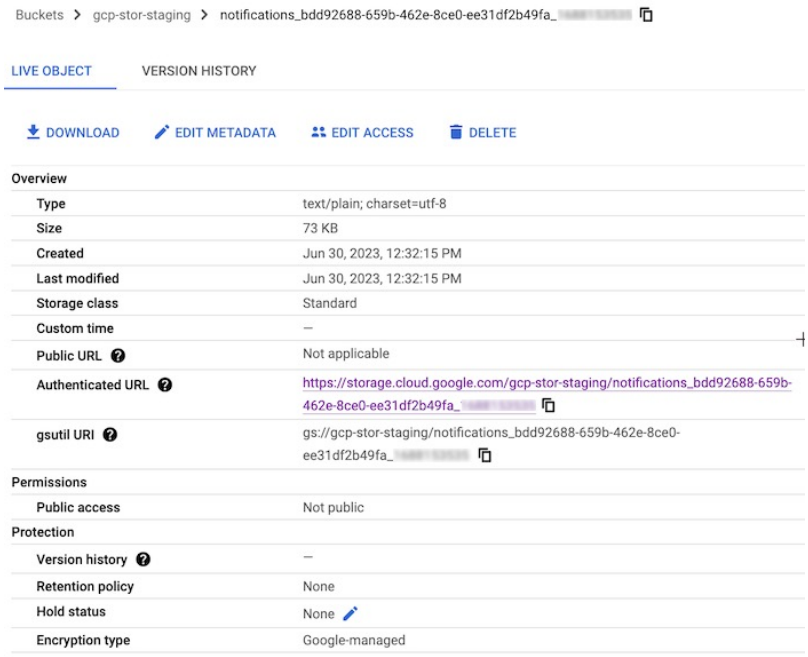
- You must have a Google Cloud Storage account and have an existing Cloud Storage Bucket where you want all alarm notification information sent to.
- You must create a service account key file (in JSON format) to allow Crosswork Cloud access to the Google Cloud Storage Bucket. You will need to upload this file as part of the Google Storage notification endpoint configuration.

Step 1 In Crosswork Cloud, click > **Global** > **Notifications** > **Google Storage** tab and click **Add Google Storage Endpoint**.

Step 2 Do the following:

a) Enter a name for the notification.
b) Toggle the option to **ENABLED**.
c) Enter the name of the Google Cloud Storage Bucket.
d) If there is a particular folder within the bucket you want notification logs to go to, enter the path.
e) Upload the JSON key file that provides access to the Google Cloud Storage.

Step 3 Click **Save**.
Example of file location and properties in Google Cloud Storage Bucket:



Note To see an example of the log file contents, see Amazon S3 and Google Storage Endpoint Notification Examples by Alarm Type, on page 94.

Configure Webex Endpoints

You can configure Crosswork Cloud to send notifications to a Webex space. This procedure describes how to create a webhook and configure the notification endpoint in the UI.

Before you begin

You must have an apphub.webex.com account and be a member of a Webex space (room) you are creating the webhook for.

Step 1 Log into https://apphub.webex.com.

Step 2 Search for **Incoming Webhooks**. The Incoming Webhooks application is listed.

Step 3 Click on the **Incoming Webhooks** application.

Step 4 On the **Incoming Webhooks** page, click **Connect**.

Step 5 If a window appears requesting permission to a number of items and you agree, click **Accept**.

Step 6 Scroll down the page and in the space provided, enter a new Webhook name and select the Webex space from the drop-down list.

Step 7 Click **Add**. The Webhook URL field is populated.

Step 8 Copy the newly created Webhook URL to use later.

Step 9 In Crosswork Cloud, click > **Global** > **Notifications**.

Step 10 Select **Webex**, then click **Create Webex Endpoint**.

Step 11 Enter a name for the endpoint.

Step 12 In the **Webhook URL** field, paste the Webhook URL you copied earlier.

```
https://webexapis.com/v1/webhooks/incoming/<new_webhook_ID>
```

Step 13 Click **Save**.

You will receive a notification in the Webex space indicating you have configured a new endpoint.

Step 14 Confirm the endpoint, and then the endpoint changes to *active* state and processes new notifications.

Configure Microsoft Team Endpoints

Follow these steps to configure Microsoft Team endpoints in Crosswork Cloud. Steps that require actions in Microsoft Teams include help links to the Microsoft support site. However, it is always best practice to search the Microsoft Teams online documentation for the latest instructions.

Step 1 In Microsoft Teams, create a team to receive the Crosswork Cloud alarm notifications.

Step 2 Create an incoming webhook and copy the unique webhook URL to use later in Crosswork Cloud.

Step 3 In Crosswork Cloud, click > **Global** > **Notifications**.

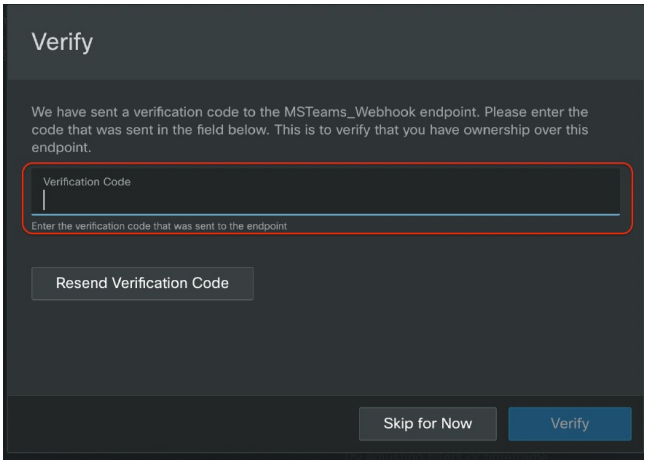
Step 4 Select **Microsoft Teams**, then click **Add Microsoft Teams Endpoint**.

Step 5 Enter a name for the endpoint.

Step 6 In the **Webhook URL** field, paste the webhook URL you copied earlier.

Step 7 Click **Save**. A verification code is sent as a message to Microsoft Teams.

Step 8 Copy the verification code from Microsoft Teams, and paste it into the Verify dialog box in Crosswork Cloud.



Step 9 Confirm the endpoint, and the endpoint changes to *active* state and processes new notifications.

Resend Confirmation Code for Endpoints

After you configure an endpoint to receive notifications from Crosswork Cloud Network Insights, you must first confirm the endpoint by entering a verification code. You can resend a verification code by following these steps:

Step 1 In the main window, click **External Routing Analytics > Configure > Notification Endpoints**.

Step 2 Click on the name of the endpoint you previously entered.

Step 3 Click **Verify**.

Crosswork Cloud Network Insights resends the verification code.

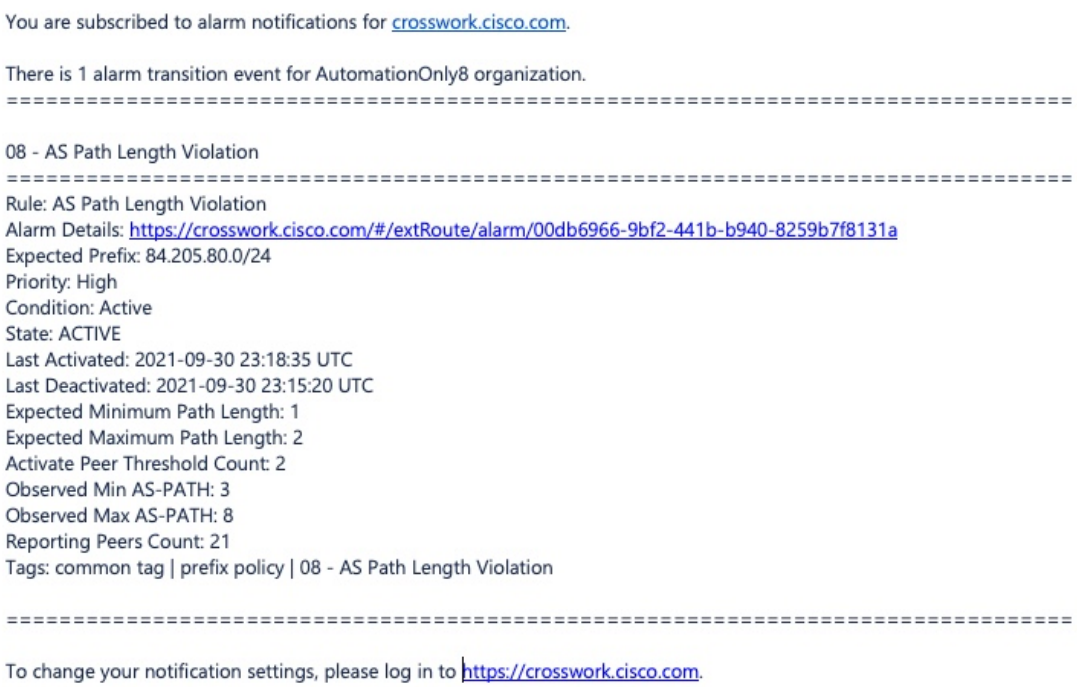
Step 4 After you receive the verification code from Crosswork Cloud Network Insights, enter the code in the **Verification Code** field, then click **Verify**.

Notification Message Examples

After you configure notification endpoints, Crosswork Cloud Network Insights sends notification messages to the endpoint you specified. The following examples show sample messages for each endpoint type.

Email Endpoint Notification Example

After you configure a notification endpoint and specify the type **Email**, when the alarm conditions are met, Crosswork Cloud Network Insights sends an email message similar to the following example:


You are subscribed to alarm notifications for crosswork.cisco.com.

There is 1 alarm transition event for AutomationOnly8 organization.
==========

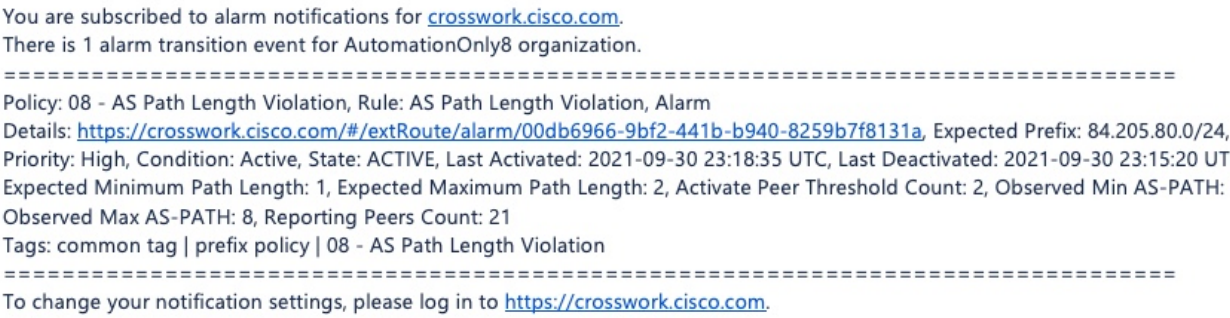
08 - AS Path Length Violation
==========
Rule: AS Path Length Violation
Alarm Details: https://crosswork.cisco.com/#/extRoute/alarm/00db6966-9bf2-441b-b940-8259b7f8131a
Expected Prefix: 84.205.80.0/24
Priority: High
Condition: Active
State: ACTIVE
Last Activated: 2021-09-30 23:18:35 UTC
Last Deactivated: 2021-09-30 23:15:20 UTC
Expected Minimum Path Length: 1
Expected Maximum Path Length: 2
Activate Peer Threshold Count: 2
Observed Min AS-PATH: 3
Observed Max AS-PATH: 8
Reporting Peers Count: 21
Tags: common tag | prefix policy | 08 - AS Path Length Violation

==========

To change your notification settings, please log in to https://crosswork.cisco.com.

Slack Endpoint Notification Example

After you configure a notification endpoint and specify the type **Slack**, when the alarm conditions are met, Crosswork Cloud Network Insights sends a Slack message similar to the following example:


You are subscribed to alarm notifications for crosswork.cisco.com.
There is 1 alarm transition event for AutomationOnly8 organization.
==========
Policy: 08 - AS Path Length Violation, Rule: AS Path Length Violation, Alarm
Details: https://crosswork.cisco.com/#/extRoute/alarm/00db6966-9bf2-441b-b940-8259b7f8131a, Expected Prefix: 84.205.80.0/24,
Priority: High, Condition: Active, State: ACTIVE, Last Activated: 2021-09-30 23:18:35 UTC, Last Deactivated: 2021-09-30 23:15:20 UT
Expected Minimum Path Length: 1, Expected Maximum Path Length: 2, Activate Peer Threshold Count: 2, Observed Min AS-PATH:
Observed Max AS-PATH: 8, Reporting Peers Count: 21
Tags: common tag | prefix policy | 08 - AS Path Length Violation
==========
To change your notification settings, please log in to https://crosswork.cisco.com.

Microsoft Teams Endpoint Notification Example

After you configure a notification endpoint and specify the type **Microsoft Teams**, when the alarm conditions are met, Crosswork Cloud Network Insights sends a message similar to the following example:

You are subscribed to alarm notifications for crosswork.cisco.com.
There is 1 alarm transition event for AutomationOnly8 organization.

Policy: 08 - AS Path Length Violation, Rule: AS Path Length Violation, Alarm
Details: https://crosswork.cisco.com/#/extRoute/alarm/00db6966-9bf2-441b-b940-8259b7f8131a, Expected Prefix: 84.205.80.0/24,
Priority: High, Condition: Active, State: ACTIVE, Last Activated: 2021-09-30 23:18:35 UTC, Last Deactivated: 2021-09-30 23:15:20 UTC,
Expected Minimum Path Length: 1, Expected Maximum Path Length: 2, Activate Peer Threshold Count: 2, Observed Min AS-PATH: 3,
Observed Max AS-PATH: 8, Reporting Peers Count: 21
Tags: common tag | prefix policy | 08 - AS Path Length Violation

==========

To change your notification settings, please log in to https://crosswork.cisco.com.

Cisco Webex Endpoint Notification Example

After you configure a notification endpoint and specify the type **Webex**, when the alarm conditions are met, Crosswork Cloud sends a Webex message similar to the following example:

You are subscribed to alarm notifications for crosswork.cisco.com.
There is 1 alarm transition event for AutomationOnly8 organization.
==========

Policy: 08 - AS Path Length Violation, Rule: AS Path Length Violation, Alarm
Details: https://crosswork.cisco.com/#/extRoute/alarm/00db6966-9bf2-441b-b940-8259b7f8131a, Expected Prefix: 84.205.80.0/24,
Priority: High, Condition: Active, State: ACTIVE, Last Activated: 2021-09-30 23:18:35 UTC, Last Deactivated: 2021-09-30 23:15:20 UTC,
Expected Minimum Path Length: 1, Expected Maximum Path Length: 2, Activate Peer Threshold Count: 2, Observed Min AS-PATH: 3,
Observed Max AS-PATH: 8, Reporting Peers Count: 21
Tags: common tag | prefix policy | 08 - AS Path Length Violation

==========

To change your notification settings, please log in to https://crosswork.cisco.com.

Amazon S3 and Google Storage Endpoint Notification Examples by Alarm Type

The following sections contain log message examples of Amazon S3 and Google Storage notifications for each alarm type.

AS Origin Violation Example

The following is an Amazon S3 and Google Storage notification log message example for an **AS Origin Violation** alarm.


```
{
  "activatedAt": "2023-02-04T03:02:19Z",
  "alarmId": "04aa5831-7e62-45cb-a123-3d5e9c019330",
  "clearedAt": "2023-02-04T03:01:41Z",
  "expected": {
    "numPeersToClear": 1,
    "numPeersToTrigger": 2,
    "originAsns": [
      1523
    ]
  },
  "monitoredPrefix": "31.1.1.0/24",
  "observed": {
```

```
  "allViolationPeers": [
    {
      "asn": 6008,
      "at": "2023-02-04T03:00:58Z",
      "peerId": 21
    },
    {
      "asn": 6009,
      "at": "2023-02-04T03:00:58Z",
      "peerId": 22
    },
    {
      "asn": 6005,
      "at": "2023-02-04T03:00:58Z",
      "peerId": 1,
      "peerIp": "10.11.12.1"
    },
    {
      "asn": 6007,
      "at": "2023-02-04T03:00:58Z",
      "peerId": 20
    },
    {
      "asn": 6002,
      "at": "2023-02-04T03:00:58Z",
      "peerId": 4,
      "peerIp": "10.11.12.4"
    },
    {
      "asn": 6004,
      "at": "2023-02-04T03:00:58Z",
      "peerId": 2,
      "peerIp": "10.11.12.2"
    },
    {
      "asn": 6001,
      "at": "2023-02-04T03:00:58Z",
      "peerId": 5,
      "peerIp": "10.11.12.5"
    },
    {
      "asn": 6000,
      "at": "2023-02-04T03:00:58Z",
      "peerId": 7,
      "peerIp": "10.31.32.1"
    },
    {
      "asn": 6006,
      "at": "2023-02-04T03:00:58Z",
      "peerId": 19
    },
    {
      "asn": 6003,
      "at": "2023-02-04T03:00:58Z",
      "peerId": 3,
      "peerIp": "10.11.12.3"
    }
  ],
  "allViolationPeersCount": 10
},
"orgName": "AutomationOnly5",
"policyId": "963b86db-329d-4cba-a38a-3fc19ddd330d",
"policyName": "02 - AS Origin Violation",
"rule": "ALARM_RULE_AS_ORIGIN_VIOLATION",
```

```
  "severity": "ALARM_SEVERITY_RED",
  "state": "ALARM_STATE_ACTIVE",
  "tags": [
    "common tag",
    "prefix policy",
    "02 - AS Origin Violation"
  ],
  "transitionedAt": "2023-02-04T03:02:19Z"
}
{
  "activatedAt": "2023-02-04T03:02:19Z",
  "alarmId": "9ea271fb-1976-450f-b653-d3d188426b6e",
  "clearedAt": "2023-02-04T03:01:42Z",
  "expected": {
    "numPeersToClear": 1,
    "numPeersToTrigger": 2,
    "originAsns": [
      1523
    ]
  },
  "monitoredPrefix": "2002:1f01:100::/48",
  "observed": {
    "allViolationPeers": [
      {
        "asn": 6009,
        "at": "2023-02-04T03:00:58Z",
        "peerId": 30
      },
      {
        "asn": 6004,
        "at": "2023-02-04T03:00:58Z",
        "peerId": 25
      },
      {
        "asn": 6001,
        "at": "2023-02-04T03:00:58Z",
        "peerId": 23
      },
      {
        "asn": 6006,
        "at": "2023-02-04T03:00:58Z",
        "peerId": 27
      },
      {
        "asn": 6000,
        "at": "2023-02-04T03:00:58Z",
        "peerId": 8,
        "peerIp": "2000::30:100:10"
      },
      {
        "asn": 6003,
        "at": "2023-02-04T03:00:58Z",
        "peerId": 24
      },
      {
        "asn": 6005,
        "at": "2023-02-04T03:00:58Z",
        "peerId": 26
      },
      {
        "asn": 6008,
        "at": "2023-02-04T03:00:58Z",
        "peerId": 29
      },
```

```
      {
        "asn": 6007,
        "at": "2023-02-04T03:00:58Z",
        "peerId": 28
      },
      {
        "asn": 6011,
        "at": "2023-02-04T03:00:58Z",
        "peerId": 32
      },
      {
        "asn": 6002,
        "at": "2023-02-04T03:00:58Z",
        "peerId": 6,
        "peerIp": "2000::20:100:10"
      },
      {
        "asn": 6010,
        "at": "2023-02-04T03:00:58Z",
        "peerId": 31
      }
    ],
    "allViolationPeersCount": 12
  },
  "orgName": "AutomationOnly5",
  "policyId": "963b86db-329d-4cba-a38a-3fc19ddd330d",
  "policyName": "02 - AS Origin Violation",
  "rule": "ALARM_RULE_AS_ORIGIN_VIOLATION",
  "severity": "ALARM_SEVERITY_RED",
  "state": "ALARM_STATE_ACTIVE",
  "tags": [
    "common tag",
    "prefix policy",
    "02 - AS Origin Violation"
  ],
  "transitionedAt": "2023-02-04T03:02:19Z"
}
```


AS Path Length Violation Example

The following is an Amazon S3 and Google Storage notification log message example for an **AS Path Length Violation** alarm.


```
{
  "activatedAt": "2023-02-04T03:09:32Z",
  "alarmId": "38a07db7-776e-4b4a-a186-b7d4bd9b045c",
  "clearedAt": "2023-02-04T03:08:53Z",
  "expected": {
    "maxAsPathLength": 2,
    "minAsPathLength": 1,
    "numPeersToClear": 1,
    "numPeersToTrigger": 2
  },
  "monitoredPrefix": "145.25.0.0/16",
  "observed": {
    "allViolationPeers": [
      {
        "asPath": [
          902,
          602,
          22
        ],
        "asPathLength": 3,
        "asn": 22,
```

```
    "at": "2023-02-04T03:06:32Z",
    "peerId": 1,
    "peerIp": "10.11.12.1"
  },
  {
    "asPath": [
      902,
      602,
      22
    ],
    "asPathLength": 3,
    "asn": 22,
    "at": "2023-02-04T03:06:32Z",
    "peerId": 19
  },
  {
    "asPath": [
      902,
      602,
      22
    ],
    "asPathLength": 3,
    "asn": 22,
    "at": "2023-02-04T03:06:32Z",
    "peerId": 2,
    "peerIp": "10.11.12.2"
  },
  {
    "asPath": [
      902,
      602,
      22
    ],
    "asPathLength": 3,
    "asn": 22,
    "at": "2023-02-04T03:06:32Z",
    "peerId": 20
  },
  {
    "asPath": [
      902,
      602,
      22
    ],
    "asPathLength": 3,
    "asn": 22,
    "at": "2023-02-04T03:06:32Z",
    "peerId": 21
  },
  {
    "asPath": [
      902,
      602,
      22
    ],
    "asPathLength": 3,
    "asn": 22,
    "at": "2023-02-04T03:06:32Z",
    "peerId": 22
  },
  {
    "asPath": [
      902,
      602,
```

```
            22
          ],
          "asPathLength": 3,
          "asn": 22,
          "at": "2023-02-04T03:06:32Z",
          "peerId": 3,
          "peerIp": "10.11.12.3"
        },
        {
          "asPath": [
            902,
            602,
            22
          ],
          "asPathLength": 3,
          "asn": 22,
          "at": "2023-02-04T03:06:32Z",
          "peerId": 4,
          "peerIp": "10.11.12.4"
        },
        {
          "asPath": [
            902,
            602,
            22
          ],
          "asPathLength": 3,
          "asn": 22,
          "at": "2023-02-04T03:06:32Z",
          "peerId": 5,
          "peerIp": "10.11.12.5"
        },
        {
          "asPath": [
            902,
            602,
            22
          ],
          "asPathLength": 3,
          "asn": 22,
          "at": "2023-02-04T03:06:32Z",
          "peerId": 7,
          "peerIp": "10.31.32.1"
        }
      ],
      "allViolationPeersCount": 10
    },
    "orgName": "AutomationOnly5",
    "policyId": "bc4298d2-1a52-4339-83e8-1d8932e1fe61",
    "policyName": "03 - AS Path Length Violation",
    "rule": "ALARM_RULE_AS_PATH_LENGTH_VIOLATION",
    "severity": "ALARM_SEVERITY_RED",
    "state": "ALARM_STATE_ACTIVE",
    "tags": [
      "common tag",
      "prefix policy",
      "03 - AS Path Length Violation"
    ],
    "transitionedAt": "2023-02-04T03:09:32Z"
}
{
    "activatedAt": "2023-02-04T03:09:32Z",
    "alarmId": "e44e6834-7877-435c-9068-169e56cae5aa",
    "clearedAt": "2023-02-04T03:08:53Z",
```

```
"expected": {
  "maxAsPathLength": 2,
  "minAsPathLength": 1,
  "numPeersToClear": 1,
  "numPeersToTrigger": 2
},
"monitoredPrefix": "2002:9119::/48",
"observed": {
  "allViolationPeers": [
    {
      "asPath": [
        902,
        602,
        22
      ],
      "asPathLength": 3,
      "asn": 22,
      "at": "2023-02-04T03:06:32Z",
      "peerId": 23
    },
    {
      "asPath": [
        902,
        602,
        22
      ],
      "asPathLength": 3,
      "asn": 22,
      "at": "2023-02-04T03:06:32Z",
      "peerId": 24
    },
    {
      "asPath": [
        902,
        602,
        22
      ],
      "asPathLength": 3,
      "asn": 22,
      "at": "2023-02-04T03:06:32Z",
      "peerId": 25
    },
    {
      "asPath": [
        902,
        602,
        22
      ],
      "asPathLength": 3,
      "asn": 22,
      "at": "2023-02-04T03:06:32Z",
      "peerId": 26
    },
    {
      "asPath": [
        902,
        602,
        22
      ],
      "asPathLength": 3,
      "asn": 22,
      "at": "2023-02-04T03:06:32Z",
      "peerId": 27
    },
```

```
{
  "asPath": [
    902,
    602,
    22
  ],
  "asPathLength": 3,
  "asn": 22,
  "at": "2023-02-04T03:06:32Z",
  "peerId": 28
},
{
  "asPath": [
    902,
    602,
    22
  ],
  "asPathLength": 3,
  "asn": 22,
  "at": "2023-02-04T03:06:32Z",
  "peerId": 29
},
{
  "asPath": [
    902,
    602,
    22
  ],
  "asPathLength": 3,
  "asn": 22,
  "at": "2023-02-04T03:06:32Z",
  "peerId": 30
},
{
  "asPath": [
    902,
    602,
    22
  ],
  "asPathLength": 3,
  "asn": 22,
  "at": "2023-02-04T03:06:32Z",
  "peerId": 31
},
{
  "asPath": [
    902,
    602,
    22
  ],
  "asPathLength": 3,
  "asn": 22,
  "at": "2023-02-04T03:06:32Z",
  "peerId": 32
},
{
  "asPath": [
    902,
    602,
    22
  ],
  "asPathLength": 3,
  "asn": 22,
  "at": "2023-02-04T03:06:32Z",
```

```
        "peerId": 6,
        "peerIp": "2000::20:100:10"
      },
      {
        "asPath": [
          902,
          602,
          22
        ],
        "asPathLength": 3,
        "asn": 22,
        "at": "2023-02-04T03:06:32Z",
        "peerId": 8,
        "peerIp": "2000::30:100:10"
      }
    ],
    "allViolationPeersCount": 12
  },
  "orgName": "AutomationOnly5",
  "policyId": "bc4298d2-1a52-4339-83e8-1d8932e1fe61",
  "policyName": "03 - AS Path Length Violation",
  "rule": "ALARM_RULE_AS_PATH_LENGTH_VIOLATION",
  "severity": "ALARM_SEVERITY_RED",
  "state": "ALARM_STATE_ACTIVE",
  "tags": [
    "common tag",
    "prefix policy",
    "03 - AS Path Length Violation"
  ],
  "transitionedAt": "2023-02-04T03:09:32Z"
}
```


DNS Root Server Withdrawal Example

The following is an Amazon S3 and Google Storage notification log message example for a **DNS Root Server Withdrawal** alarm.


```
{
  "activatedAt": "2023-02-04T06:16:17Z",
  "alarmId": "5161f679-8e4e-4b95-a979-1788b3444136",
  "monitoredPeer": {
    "peerIp": "2000::30:100:10",
    "peerName": "Root DNS IPv6",
    "sessionId": "9b3f0207-a484-465b-886b-0c8bbcefb8bc"
  },
  "observed": {
    "withdrawnPrefix": "2001:503:ba3e::/48"
  },
  "orgName": "AutomationOnly5",
  "policyId": "3fb1473d-a1cb-43f2-b232-6a3cb470051b",
  "policyName": "20 - DNS Root Server Withdrawal",
  "rule": "ALARM_RULE_DNS_ROOT_SERVER_WITHDRAWAL",
  "severity": "ALARM_SEVERITY_RED",
  "state": "ALARM_STATE_ACTIVE",
  "transitionedAt": "2023-02-04T06:16:17Z"
}
{
  "activatedAt": "2023-02-04T06:16:17Z",
  "alarmId": "b87dc535-7151-4728-90f2-0b24b979d4b8",
  "monitoredPeer": {
    "peerIp": "10.31.32.1",
    "peerName": "Root DNS IPv4",
    "sessionId": "c5dcf2d2-99b7-4565-8b29-9b30f20ed2f7"
  },
```

```
  "observed": {
    "withdrawnPrefix": "198.41.0.0/24"
  },
  "orgName": "AutomationOnly5",
  "policyId": "3fb1473d-a1cb-43f2-b232-6a3cb470051b",
  "policyName": "20 - DNS Root Server Withdrawal",
  "rule": "ALARM_RULE_DNS_ROOT_SERVER_WITHDRAWAL",
  "severity": "ALARM_SEVERITY_RED",
  "state": "ALARM_STATE_ACTIVE",
  "transitionedAt": "2023-02-04T06:16:17Z"
}
```


New AS Path Edge Example

The following is an Amazon S3 notification and Google Storage log message example for a **New AS Path Edge** alarm.


```
{
  "activatedAt": "2023-02-04T03:11:17Z",
  "alarmId": "4b9eb669-774d-4a6d-bed5-d559248953e8",
  "expected": {
    "numPeersToTrigger": 1
  },
  "monitoredPrefix": "88.88.109.0/24",
  "observed": {
    "allViolationPeers": [
      {
        "asPath": [
          916,
          700,
          620,
          36
        ],
        "asn": 36,
        "at": "2023-02-04T01:34:59Z",
        "peerId": 1,
        "peerIp": "10.11.12.1",
        "suspiciousEdges": [
          {
            "edgeId": {
              "fromAs": 36,
              "toAs": 620
            },
            "firstSeen": "2023-02-04T01:34:59Z",
            "lastSeen": "2023-02-04T01:34:59Z",
            "peerCount": 2,
            "prefixCount": 2,
            "prefixList": [
              "2002:5858:6d00::/48",
              "88.88.109.0/24"
            ]
          },
          {
            "edgeId": {
              "fromAs": 620,
              "toAs": 700
            },
            "firstSeen": "2023-02-04T01:34:59Z",
            "lastSeen": "2023-02-04T01:34:59Z",
            "peerCount": 2,
            "prefixCount": 2,
            "prefixList": [
              "88.88.109.0/24",
              "2002:5858:6d00::/48"
```

```
      ]
    }
  ]
},
{
  "asPath": [
    916,
    700,
    621,
    36
  ],
  "asn": 36,
  "at": "2023-02-04T01:34:59Z",
  "peerId": 19,
  "suspiciousEdges": [
    {
      "edgeId": {
        "fromAs": 36,
        "toAs": 621
      },
      "firstSeen": "2023-02-04T01:34:59Z",
      "lastSeen": "2023-02-04T01:34:59Z",
      "peerCount": 2,
      "prefixCount": 2,
      "prefixList": [
        "88.88.109.0/24",
        "2002:5858:6d00::/48"
      ]
    },
    {
      "edgeId": {
        "fromAs": 621,
        "toAs": 700
      },
      "firstSeen": "2023-02-04T01:34:59Z",
      "lastSeen": "2023-02-04T01:34:59Z",
      "peerCount": 2,
      "prefixCount": 2,
      "prefixList": [
        "88.88.109.0/24",
        "2002:5858:6d00::/48"
      ]
    }
  ]
},
{
  "asPath": [
    916,
    700,
    619,
    36
  ],
  "asn": 36,
  "at": "2023-02-04T01:34:59Z",
  "peerId": 2,
  "peerIp": "10.11.12.2",
  "suspiciousEdges": [
    {
      "edgeId": {
        "fromAs": 36,
        "toAs": 619
      },
      "firstSeen": "2023-02-04T01:34:59Z",
      "lastSeen": "2023-02-04T01:34:59Z",
```

```
      "peerCount": 2,
      "prefixCount": 2,
      "prefixList": [
        "2002:5858:6d00::/48",
        "88.88.109.0/24"
      ]
    },
    {
      "edgeId": {
        "fromAs": 619,
        "toAs": 700
      },
      "firstSeen": "2023-02-04T01:34:59Z",
      "lastSeen": "2023-02-04T01:34:59Z",
      "peerCount": 2,
      "prefixCount": 2,
      "prefixList": [
        "88.88.109.0/24",
        "2002:5858:6d00::/48"
      ]
    }
  ]
},
{
  "asPath": [
    916,
    700,
    622,
    36
  ],
  "asn": 36,
  "at": "2023-02-04T01:34:59Z",
  "peerId": 20,
  "suspiciousEdges": [
    {
      "edgeId": {
        "fromAs": 36,
        "toAs": 622
      },
      "firstSeen": "2023-02-04T01:34:59Z",
      "lastSeen": "2023-02-04T01:34:59Z",
      "peerCount": 2,
      "prefixCount": 2,
      "prefixList": [
        "88.88.109.0/24",
        "2002:5858:6d00::/48"
      ]
    },
    {
      "edgeId": {
        "fromAs": 622,
        "toAs": 700
      },
      "firstSeen": "2023-02-04T01:34:59Z",
      "lastSeen": "2023-02-04T01:34:59Z",
      "peerCount": 2,
      "prefixCount": 2,
      "prefixList": [
        "88.88.109.0/24",
        "2002:5858:6d00::/48"
      ]
    }
  ]
},
```

```
{
  "asPath": [
    916,
    700,
    623,
    36
  ],
  "asn": 36,
  "at": "2023-02-04T01:34:59Z",
  "peerId": 21,
  "suspiciousEdges": [
    {
      "edgeId": {
        "fromAs": 36,
        "toAs": 623
      },
      "firstSeen": "2023-02-04T01:34:59Z",
      "lastSeen": "2023-02-04T01:34:59Z",
      "peerCount": 2,
      "prefixCount": 2,
      "prefixList": [
        "2002:5858:6d00::/48",
        "88.88.109.0/24"
      ]
    },
    {
      "edgeId": {
        "fromAs": 623,
        "toAs": 700
      },
      "firstSeen": "2023-02-04T01:34:59Z",
      "lastSeen": "2023-02-04T01:34:59Z",
      "peerCount": 2,
      "prefixCount": 2,
      "prefixList": [
        "88.88.109.0/24",
        "2002:5858:6d00::/48"
      ]
    }
  ]
},
{
  "asPath": [
    916,
    700,
    624,
    36
  ],
  "asn": 36,
  "at": "2023-02-04T01:34:59Z",
  "peerId": 22,
  "suspiciousEdges": [
    {
      "edgeId": {
        "fromAs": 36,
        "toAs": 624
      },
      "firstSeen": "2023-02-04T01:34:59Z",
      "lastSeen": "2023-02-04T01:34:59Z",
      "peerCount": 2,
      "prefixCount": 2,
      "prefixList": [
        "88.88.109.0/24",
        "2002:5858:6d00::/48"
```

```
      ]
    },
    {
      "edgeId": {
        "fromAs": 624,
        "toAs": 700
      },
      "firstSeen": "2023-02-04T01:34:59Z",
      "lastSeen": "2023-02-04T01:34:59Z",
      "peerCount": 2,
      "prefixCount": 2,
      "prefixList": [
        "88.88.109.0/24",
        "2002:5858:6d00::/48"
      ]
    }
  ]
},
{
  "asPath": [
    916,
    700,
    618,
    36
  ],
  "asn": 36,
  "at": "2023-02-04T01:34:59Z",
  "peerId": 3,
  "peerIp": "10.11.12.3",
  "suspiciousEdges": [
    {
      "edgeId": {
        "fromAs": 36,
        "toAs": 618
      },
      "firstSeen": "2023-02-04T01:34:59Z",
      "lastSeen": "2023-02-04T01:34:59Z",
      "peerCount": 2,
      "prefixCount": 2,
      "prefixList": [
        "88.88.109.0/24",
        "2002:5858:6d00::/48"
      ]
    },
    {
      "edgeId": {
        "fromAs": 618,
        "toAs": 700
      },
      "firstSeen": "2023-02-04T01:34:59Z",
      "lastSeen": "2023-02-04T01:34:59Z",
      "peerCount": 2,
      "prefixCount": 2,
      "prefixList": [
        "88.88.109.0/24",
        "2002:5858:6d00::/48"
      ]
    }
  ]
},
{
  "asPath": [
    916,
    700,
```

```
      617,
      36
    ],
    "asn": 36,
    "at": "2023-02-04T01:34:59Z",
    "peerId": 4,
    "peerIp": "10.11.12.4",
    "suspiciousEdges": [
      {
        "edgeId": {
          "fromAs": 36,
          "toAs": 617
        },
        "firstSeen": "2023-02-04T01:34:59Z",
        "lastSeen": "2023-02-04T01:34:59Z",
        "peerCount": 2,
        "prefixCount": 2,
        "prefixList": [
          "88.88.109.0/24",
          "2002:5858:6d00::/48"
        ]
      },
      {
        "edgeId": {
          "fromAs": 617,
          "toAs": 700
        },
        "firstSeen": "2023-02-04T01:34:59Z",
        "lastSeen": "2023-02-04T01:34:59Z",
        "peerCount": 2,
        "prefixCount": 2,
        "prefixList": [
          "88.88.109.0/24",
          "2002:5858:6d00::/48"
        ]
      }
    ]
  },
  {
    "asPath": [
      916,
      700,
      616,
      36
    ],
    "asn": 36,
    "at": "2023-02-04T01:34:59Z",
    "peerId": 5,
    "peerIp": "10.11.12.5",
    "suspiciousEdges": [
      {
        "edgeId": {
          "fromAs": 36,
          "toAs": 616
        },
        "firstSeen": "2023-02-04T01:34:59Z",
        "lastSeen": "2023-02-04T01:34:59Z",
        "peerCount": 2,
        "prefixCount": 2,
        "prefixList": [
          "88.88.109.0/24",
          "2002:5858:6d00::/48"
        ]
      },
```

```
          {
            "edgeId": {
              "fromAs": 616,
              "toAs": 700
            },
            "firstSeen": "2023-02-04T01:34:59Z",
            "lastSeen": "2023-02-04T01:34:59Z",
            "peerCount": 2,
            "prefixCount": 2,
            "prefixList": [
              "2002:5858:6d00::/48",
              "88.88.109.0/24"
            ]
          }
        ]
      },
      {
        "asPath": [
          916,
          700,
          615,
          36
        ],
        "asn": 36,
        "at": "2023-02-04T01:34:59Z",
        "peerId": 7,
        "peerIp": "10.31.32.1",
        "suspiciousEdges": [
          {
            "edgeId": {
              "fromAs": 36,
              "toAs": 615
            },
            "firstSeen": "2023-02-04T01:34:59Z",
            "lastSeen": "2023-02-04T01:34:59Z",
            "peerCount": 2,
            "prefixCount": 2,
            "prefixList": [
              "88.88.109.0/24",
              "2002:5858:6d00::/48"
            ]
          },
          {
            "edgeId": {
              "fromAs": 615,
              "toAs": 700
            },
            "firstSeen": "2023-02-04T01:34:59Z",
            "lastSeen": "2023-02-04T01:34:59Z",
            "peerCount": 2,
            "prefixCount": 2,
            "prefixList": [
              "88.88.109.0/24",
              "2002:5858:6d00::/48"
            ]
          }
        ]
      }
    ],
    "allViolationPeersCount": 10
  },
  "orgName": "AutomationOnly5",
  "policyId": "3755ed13-6498-4cc6-9798-a1264d03b402",
  "policyName": "04 - New AS Path Edge",
```

```
  "rule": "ALARM_RULE_NEW_AS_PATH_EDGE",
  "severity": "ALARM_SEVERITY_RED",
  "state": "ALARM_STATE_ACTIVE",
  "tags": [
    "common tag",
    "prefix policy",
    "04 - New AS Path Edge"
  ],
  "transitionedAt": "2023-02-04T03:11:17Z"
}
{
  "activatedAt": "2023-02-04T03:11:17Z",
  "alarmId": "9a1ab970-144b-4256-a864-4eb26e698844",
  "expected": {
    "numPeersToTrigger": 1
  },
  "monitoredPrefix": "2002:5858:6d00::/48",
  "observed": {
    "allViolationPeers": [
      {
        "asPath": [
          916,
          700,
          616,
          36
        ],
        "asn": 36,
        "at": "2023-02-04T01:34:59Z",
        "peerId": 23,
        "suspiciousEdges": [
          {
            "edgeId": {
              "fromAs": 36,
              "toAs": 616
            },
            "firstSeen": "2023-02-04T01:34:59Z",
            "lastSeen": "2023-02-04T01:34:59Z",
            "peerCount": 2,
            "prefixCount": 2,
            "prefixList": [
              "88.88.109.0/24",
              "2002:5858:6d00::/48"
            ]
          },
          {
            "edgeId": {
              "fromAs": 616,
              "toAs": 700
            },
            "firstSeen": "2023-02-04T01:34:59Z",
            "lastSeen": "2023-02-04T01:34:59Z",
            "peerCount": 2,
            "prefixCount": 2,
            "prefixList": [
              "2002:5858:6d00::/48",
              "88.88.109.0/24"
            ]
          }
        ]
      },
      {
        "asPath": [
          916,
          700,
```

```
      618,
      36
    ],
    "asn": 36,
    "at": "2023-02-04T01:34:59Z",
    "peerId": 24,
    "suspiciousEdges": [
      {
        "edgeId": {
          "fromAs": 36,
          "toAs": 618
        },
        "firstSeen": "2023-02-04T01:34:59Z",
        "lastSeen": "2023-02-04T01:34:59Z",
        "peerCount": 2,
        "prefixCount": 2,
        "prefixList": [
          "88.88.109.0/24",
          "2002:5858:6d00::/48"
        ]
      },
      {
        "edgeId": {
          "fromAs": 618,
          "toAs": 700
        },
        "firstSeen": "2023-02-04T01:34:59Z",
        "lastSeen": "2023-02-04T01:34:59Z",
        "peerCount": 2,
        "prefixCount": 2,
        "prefixList": [
          "88.88.109.0/24",
          "2002:5858:6d00::/48"
        ]
      }
    ]
  },
  {
    "asPath": [
      916,
      700,
      619,
      36
    ],
    "asn": 36,
    "at": "2023-02-04T01:34:59Z",
    "peerId": 25,
    "suspiciousEdges": [
      {
        "edgeId": {
          "fromAs": 36,
          "toAs": 619
        },
        "firstSeen": "2023-02-04T01:34:59Z",
        "lastSeen": "2023-02-04T01:34:59Z",
        "peerCount": 2,
        "prefixCount": 2,
        "prefixList": [
          "2002:5858:6d00::/48",
          "88.88.109.0/24"
        ]
      },
      {
        "edgeId": {
```

```
        "fromAs": 619,
        "toAs": 700
      },
      "firstSeen": "2023-02-04T01:34:59Z",
      "lastSeen": "2023-02-04T01:34:59Z",
      "peerCount": 2,
      "prefixCount": 2,
      "prefixList": [
        "88.88.109.0/24",
        "2002:5858:6d00::/48"
      ]
    }
  ]
},
{
  "asPath": [
    916,
    700,
    620,
    36
  ],
  "asn": 36,
  "at": "2023-02-04T01:34:59Z",
  "peerId": 26,
  "suspiciousEdges": [
    {
      "edgeId": {
        "fromAs": 36,
        "toAs": 620
      },
      "firstSeen": "2023-02-04T01:34:59Z",
      "lastSeen": "2023-02-04T01:34:59Z",
      "peerCount": 2,
      "prefixCount": 2,
      "prefixList": [
        "2002:5858:6d00::/48",
        "88.88.109.0/24"
      ]
    },
    {
      "edgeId": {
        "fromAs": 620,
        "toAs": 700
      },
      "firstSeen": "2023-02-04T01:34:59Z",
      "lastSeen": "2023-02-04T01:34:59Z",
      "peerCount": 2,
      "prefixCount": 2,
      "prefixList": [
        "88.88.109.0/24",
        "2002:5858:6d00::/48"
      ]
    }
  ]
},
{
  "asPath": [
    916,
    700,
    621,
    36
  ],
  "asn": 36,
  "at": "2023-02-04T01:34:59Z",
```

```
  "peerId": 27,
  "suspiciousEdges": [
    {
      "edgeId": {
        "fromAs": 36,
        "toAs": 621
      },
      "firstSeen": "2023-02-04T01:34:59Z",
      "lastSeen": "2023-02-04T01:34:59Z",
      "peerCount": 2,
      "prefixCount": 2,
      "prefixList": [
        "88.88.109.0/24",
        "2002:5858:6d00::/48"
      ]
    },
    {
      "edgeId": {
        "fromAs": 621,
        "toAs": 700
      },
      "firstSeen": "2023-02-04T01:34:59Z",
      "lastSeen": "2023-02-04T01:34:59Z",
      "peerCount": 2,
      "prefixCount": 2,
      "prefixList": [
        "88.88.109.0/24",
        "2002:5858:6d00::/48"
      ]
    }
  ]
},
{
  "asPath": [
    916,
    700,
    622,
    36
  ],
  "asn": 36,
  "at": "2023-02-04T01:34:59Z",
  "peerId": 28,
  "suspiciousEdges": [
    {
      "edgeId": {
        "fromAs": 36,
        "toAs": 622
      },
      "firstSeen": "2023-02-04T01:34:59Z",
      "lastSeen": "2023-02-04T01:34:59Z",
      "peerCount": 2,
      "prefixCount": 2,
      "prefixList": [
        "88.88.109.0/24",
        "2002:5858:6d00::/48"
      ]
    },
    {
      "edgeId": {
        "fromAs": 622,
        "toAs": 700
      },
      "firstSeen": "2023-02-04T01:34:59Z",
      "lastSeen": "2023-02-04T01:34:59Z",
```

```
        "peerCount": 2,
        "prefixCount": 2,
        "prefixList": [
          "88.88.109.0/24",
          "2002:5858:6d00::/48"
        ]
      }
    ]
  },
  {
    "asPath": [
      916,
      700,
      623,
      36
    ],
    "asn": 36,
    "at": "2023-02-04T01:34:59Z",
    "peerId": 29,
    "suspiciousEdges": [
      {
        "edgeId": {
          "fromAs": 36,
          "toAs": 623
        },
        "firstSeen": "2023-02-04T01:34:59Z",
        "lastSeen": "2023-02-04T01:34:59Z",
        "peerCount": 2,
        "prefixCount": 2,
        "prefixList": [
          "2002:5858:6d00::/48",
          "88.88.109.0/24"
        ]
      },
      {
        "edgeId": {
          "fromAs": 623,
          "toAs": 700
        },
        "firstSeen": "2023-02-04T01:34:59Z",
        "lastSeen": "2023-02-04T01:34:59Z",
        "peerCount": 2,
        "prefixCount": 2,
        "prefixList": [
          "88.88.109.0/24",
          "2002:5858:6d00::/48"
        ]
      }
    ]
  },
  {
    "asPath": [
      916,
      700,
      624,
      36
    ],
    "asn": 36,
    "at": "2023-02-04T01:34:59Z",
    "peerId": 30,
    "suspiciousEdges": [
      {
        "edgeId": {
          "fromAs": 36,
```

```
        "toAs": 624
      },
      "firstSeen": "2023-02-04T01:34:59Z",
      "lastSeen": "2023-02-04T01:34:59Z",
      "peerCount": 2,
      "prefixCount": 2,
      "prefixList": [
        "88.88.109.0/24",
        "2002:5858:6d00::/48"
      ]
    },
    {
      "edgeId": {
        "fromAs": 624,
        "toAs": 700
      },
      "firstSeen": "2023-02-04T01:34:59Z",
      "lastSeen": "2023-02-04T01:34:59Z",
      "peerCount": 2,
      "prefixCount": 2,
      "prefixList": [
        "88.88.109.0/24",
        "2002:5858:6d00::/48"
      ]
    }
  ]
},
{
  "asPath": [
    916,
    700,
    625,
    36
  ],
  "asn": 36,
  "at": "2023-02-04T01:34:59Z",
  "peerId": 31,
  "suspiciousEdges": [
    {
      "edgeId": {
        "fromAs": 36,
        "toAs": 625
      },
      "firstSeen": "2023-02-04T01:34:59Z",
      "lastSeen": "2023-02-04T01:34:59Z",
      "peerCount": 1,
      "prefixCount": 1,
      "prefixList": [
        "2002:5858:6d00::/48"
      ]
    },
    {
      "edgeId": {
        "fromAs": 625,
        "toAs": 700
      },
      "firstSeen": "2023-02-04T01:34:59Z",
      "lastSeen": "2023-02-04T01:34:59Z",
      "peerCount": 1,
      "prefixCount": 1,
      "prefixList": [
        "2002:5858:6d00::/48"
      ]
    }
```

```
    ]
  },
  {
    "asPath": [
      916,
      700,
      626,
      36
    ],
    "asn": 36,
    "at": "2023-02-04T01:34:59Z",
    "peerId": 32,
    "suspiciousEdges": [
      {
        "edgeId": {
          "fromAs": 36,
          "toAs": 626
        },
        "firstSeen": "2023-02-04T01:34:59Z",
        "lastSeen": "2023-02-04T01:34:59Z",
        "peerCount": 1,
        "prefixCount": 1,
        "prefixList": [
          "2002:5858:6d00::/48"
        ]
      },
      {
        "edgeId": {
          "fromAs": 626,
          "toAs": 700
        },
        "firstSeen": "2023-02-04T01:34:59Z",
        "lastSeen": "2023-02-04T01:34:59Z",
        "peerCount": 1,
        "prefixCount": 1,
        "prefixList": [
          "2002:5858:6d00::/48"
        ]
      }
    ]
  },
  {
    "asPath": [
      916,
      700,
      617,
      36
    ],
    "asn": 36,
    "at": "2023-02-04T01:34:59Z",
    "peerId": 6,
    "peerIp": "2000::20:100:10",
    "suspiciousEdges": [
      {
        "edgeId": {
          "fromAs": 36,
          "toAs": 617
        },
        "firstSeen": "2023-02-04T01:34:59Z",
        "lastSeen": "2023-02-04T01:34:59Z",
        "peerCount": 2,
        "prefixCount": 2,
        "prefixList": [
          "88.88.109.0/24",
```

```
            "2002:5858:6d00::/48"
          ]
        },
        {
          "edgeId": {
            "fromAs": 617,
            "toAs": 700
          },
          "firstSeen": "2023-02-04T01:34:59Z",
          "lastSeen": "2023-02-04T01:34:59Z",
          "peerCount": 2,
          "prefixCount": 2,
          "prefixList": [
            "88.88.109.0/24",
            "2002:5858:6d00::/48"
          ]
        }
      ]
    },
    {
      "asPath": [
        916,
        700,
        615,
        36
      ],
      "asn": 36,
      "at": "2023-02-04T01:34:59Z",
      "peerId": 8,
      "peerIp": "2000::30:100:10",
      "suspiciousEdges": [
        {
          "edgeId": {
            "fromAs": 36,
            "toAs": 615
          },
          "firstSeen": "2023-02-04T01:34:59Z",
          "lastSeen": "2023-02-04T01:34:59Z",
          "peerCount": 2,
          "prefixCount": 2,
          "prefixList": [
            "88.88.109.0/24",
            "2002:5858:6d00::/48"
          ]
        },
        {
          "edgeId": {
            "fromAs": 615,
            "toAs": 700
          },
          "firstSeen": "2023-02-04T01:34:59Z",
          "lastSeen": "2023-02-04T01:34:59Z",
          "peerCount": 2,
          "prefixCount": 2,
          "prefixList": [
            "88.88.109.0/24",
            "2002:5858:6d00::/48"
          ]
        }
      ]
    }
  ],
  "allViolationPeersCount": 12
},
```

```
  "orgName": "AutomationOnly5",
  "policyId": "3755ed13-6498-4cc6-9798-a1264d03b402",
  "policyName": "04 - New AS Path Edge",
  "rule": "ALARM_RULE_NEW_AS_PATH_EDGE",
  "severity": "ALARM_SEVERITY_RED",
  "state": "ALARM_STATE_ACTIVE",
  "tags": [
    "common tag",
    "prefix policy",
    "04 - New AS Path Edge"
  ],
  "transitionedAt": "2023-02-04T03:11:17Z"
}
```


Parent Aggregate Change Example

The following is an Amazon S3 notification and Google Storage notification log message example for a **Parent Aggregate Change** alarm.


```
{
  "activatedAt": "2023-02-04T05:23:55Z",
  "alarmId": "928315c2-c804-47dc-bc52-e2282e605753",
  "expected": {
    "allowedAggregates": [
      "2002::/16",
      "2002::/17",
      "2002:57e8::/36"
    ],
    "numPeersToClear": 1,
    "numPeersToTrigger": 2,
    "originAsns": [
      1000
    ],
    "originAsnsUsage": "ALARM_USAGE_EXCLUDE"
  },
  "monitoredPrefix": "2002:57e8::/48",
  "observed": {
    "allViolationPeers": [
      {
        "peerId": 23
      },
      {
        "peerId": 24
      },
      {
        "peerId": 25
      },
      {
        "peerId": 26
      },
      {
        "peerId": 27
      },
      {
        "peerId": 28
      },
      {
        "peerId": 29
      },
      {
        "peerId": 30
      },
      {
        "peerId": 31
```

```
    },
    {
      "peerId": 32
    },
    {
      "peerId": 6
    },
    {
      "peerId": 8
    }
  ],
  "allViolationPeersCount": 12,
  "lastViolationPeers": [
    {
      "asn": 6002,
      "at": "2023-02-04T05:03:37Z",
      "peerId": 6,
      "peerIp": "2000::20:100:10"
    },
    {
      "asn": 6010,
      "at": "2023-02-04T05:03:37Z",
      "peerId": 31
    },
    {
      "asn": 6009,
      "at": "2023-02-04T05:03:37Z",
      "peerId": 30
    },
    {
      "asn": 6003,
      "at": "2023-02-04T05:03:37Z",
      "peerId": 24
    },
    {
      "asn": 6011,
      "at": "2023-02-04T05:03:37Z",
      "peerId": 32
    },
    {
      "asn": 6005,
      "at": "2023-02-04T05:03:37Z",
      "peerId": 26
    },
    {
      "asn": 6007,
      "at": "2023-02-04T05:03:37Z",
      "peerId": 28
    },
    {
      "asn": 6004,
      "at": "2023-02-04T05:03:37Z",
      "peerId": 25
    },
    {
      "asn": 6006,
      "at": "2023-02-04T05:03:37Z",
      "peerId": 27
    },
    {
      "asn": 6000,
      "at": "2023-02-04T05:03:37Z",
      "peerId": 8,
      "peerIp": "2000::30:100:10"
```

```
        },
        {
          "asn": 6001,
          "at": "2023-02-04T05:03:37Z",
          "peerId": 23
        },
        {
          "asn": 6008,
          "at": "2023-02-04T05:03:37Z",
          "peerId": 29
        }
      ],
      "lastViolationPeersCount": 12,
      "lastViolationPrefix": "2002:57e8::/36",
      "violationPrefixesCount": 3
    },
    "orgName": "AutomationOnly5",
    "policyId": "3dd434f4-92fe-447f-b7e8-129b09cff9da",
    "policyName": "17 - Parent Aggregate Change - Test 3",
    "rule": "ALARM_RULE_PARENT_AGGREGATE_CHANGE",
    "severity": "ALARM_SEVERITY_RED",
    "state": "ALARM_STATE_ACTIVE",
    "tags": [
      "common tag",
      "prefix policy",
      "17 - Parent Aggregate Change"
    ],
    "transitionedAt": "2023-02-04T05:23:55Z"
  }
  {
    "activatedAt": "2023-02-04T05:23:55Z",
    "alarmId": "c3d24f64-5814-463e-855f-da56545a621f",
    "expected": {
      "allowedAggregates": [
        "87.232.0.0/22"
      ],
      "numPeersToClear": 1,
      "numPeersToTrigger": 2,
      "originAsns": [
        1000
      ],
      "originAsnsUsage": "ALARM_USAGE_EXCLUDE"
    },
    "monitoredPrefix": "87.232.0.0/24",
    "observed": {
      "allViolationPeers": [
        {
          "peerId": 1
        },
        {
          "peerId": 19
        },
        {
          "peerId": 2
        },
        {
          "peerId": 20
        },
        {
          "peerId": 21
        },
        {
          "peerId": 22
        },
```

```
    {
      "peerId": 3
    },
    {
      "peerId": 4
    },
    {
      "peerId": 5
    },
    {
      "peerId": 7
    }
  ],
  "allViolationPeersCount": 10,
  "lastViolationPeers": [
    {
      "asn": 6004,
      "at": "2023-02-04T05:03:37Z",
      "peerId": 2,
      "peerIp": "10.11.12.2"
    },
    {
      "asn": 6008,
      "at": "2023-02-04T05:03:37Z",
      "peerId": 21
    },
    {
      "asn": 6009,
      "at": "2023-02-04T05:03:37Z",
      "peerId": 22
    },
    {
      "asn": 6002,
      "at": "2023-02-04T05:03:37Z",
      "peerId": 4,
      "peerIp": "10.11.12.4"
    },
    {
      "asn": 6003,
      "at": "2023-02-04T05:03:37Z",
      "peerId": 3,
      "peerIp": "10.11.12.3"
    },
    {
      "asn": 6005,
      "at": "2023-02-04T05:03:37Z",
      "peerId": 1,
      "peerIp": "10.11.12.1"
    },
    {
      "asn": 6006,
      "at": "2023-02-04T05:03:37Z",
      "peerId": 19
    },
    {
      "asn": 6001,
      "at": "2023-02-04T05:03:37Z",
      "peerId": 5,
      "peerIp": "10.11.12.5"
    },
    {
      "asn": 6000,
      "at": "2023-02-04T05:03:37Z",
      "peerId": 7,
```

```
        "peerIp": "10.31.32.1"
      },
      {
        "asn": 6007,
        "at": "2023-02-04T05:03:37Z",
        "peerId": 20
      }
    ],
    "lastViolationPeersCount": 10,
    "lastViolationPrefix": "87.232.0.0/22",
    "violationPrefixesCount": 1
  },
  "orgName": "AutomationOnly5",
  "policyId": "3dd434f4-92fe-447f-b7e8-129b09cff9da",
  "policyName": "17 - Parent Aggregate Change - Test 3",
  "rule": "ALARM_RULE_PARENT_AGGREGATE_CHANGE",
  "severity": "ALARM_SEVERITY_RED",
  "state": "ALARM_STATE_ACTIVE",
  "tags": [
    "common tag",
    "prefix policy",
    "17 - Parent Aggregate Change"
  ],
  "transitionedAt": "2023-02-04T05:23:55Z"
}
```


Peer Advertised Prefix Count Example

The following is an Amazon S3 notification and Google Storage notification log message example for a **Peer Advertised Prefix Count** alarm.


```
{
  "activatedAt": "2023-02-04T06:18:37Z",
  "alarmId": "139a7983-36ba-4d17-8371-2480290f3799",
  "expected": {
    "prefixCounts": [
      {
        "addressFamily": "ALARM_BGP_AF_IPV4",
        "maxPrefixes": 100,
        "minPrefixes": 10
      }
    ]
  },
  "monitoredPeer": {
    "ciscoPeerIp": "104.236.154.30",
    "ciscoPeerName": "RS06",
    "peerIp": "10.11.12.1",
    "peerName": "BGP-1",
    "sessionId": "de26c09c-15f6-435f-9044-c9a89fdc7bed"
  },
  "observed": {
    "prefixCounts": [
      {
        "addressFamily": "ALARM_BGP_AF_IPV4",
        "prefixCount": 2000
      }
    ]
  },
  "orgName": "AutomationOnly5",
  "policyId": "482de3d2-8550-4b84-a0ab-3b3e36f5869a",
  "policyName": "22 - Peer Advertised Prefix Count",
  "rule": "ALARM_RULE_ADVERTISED_PREFIX_COUNT",
  "severity": "ALARM_SEVERITY_RED",
  "state": "ALARM_STATE_ACTIVE",
```

```
  "transitionedAt": "2023-02-04T06:18:37Z"
}
```


Peer Down Example

The following is an Amazon S3 notification and Google Storage notification log message example for a **Peer Down** alarm.


```
{
  "activatedAt": "2023-02-04T06:17:05Z",
  "alarmId": "b654ced0-5357-4eb7-b3c9-27cbd24a8f65",
  "monitoredPeer": {
    "ciscoPeerIp": "3.21.42.66",
    "ciscoPeerName": "RS95",
    "peerIp": "10.11.12.2",
    "peerName": "BGP-2",
    "sessionId": "29651423-e603-4a11-89b7-37500e40e562"
  },
  "observed": {
    "lastUpdatedAt": "2019-10-03T22:30:00Z"
  },
  "orgName": "AutomationOnly5",
  "policyId": "ff3b620d-33a9-49c0-9e33-b99b53c55b1d",
  "policyName": "21 - Peer Down",
  "rule": "ALARM_RULE_PEER_DOWN",
  "severity": "ALARM_SEVERITY_YELLOW",
  "state": "ALARM_STATE_ACTIVE",
  "transitionedAt": "2023-02-04T06:17:05Z"
}
```


Prefix Advertisement Example

The following is an Amazon S3 notification and Google Storage notification log message example for a **Prefix Advertisement** alarm.


```
{
  "activatedAt": "2023-02-04T03:16:25Z",
  "alarmId": "79222047-4954-4b6e-a339-9d01bfb06434",
  "clearedAt": "2023-02-04T03:15:47Z",
  "expected": {
    "numPeersToClear": 1,
    "numPeersToTrigger": 2
  },
  "monitoredPrefix": "218.56.100.0/28",
  "observed": {
    "allViolationPeers": [
      {
        "asn": 20,
        "at": "2023-02-04T03:15:04Z",
        "peerId": 1,
        "peerIp": "10.11.12.1"
      },
      {
        "asn": 20,
        "at": "2023-02-04T03:15:04Z",
        "peerId": 19
      },
      {
        "asn": 20,
        "at": "2023-02-04T03:15:04Z",
        "peerId": 2,
        "peerIp": "10.11.12.2"
      },
```

```
        {
          "asn": 20,
          "at": "2023-02-04T03:15:04Z",
          "peerId": 20
        },
        {
          "asn": 20,
          "at": "2023-02-04T03:15:04Z",
          "peerId": 21
        },
        {
          "asn": 20,
          "at": "2023-02-04T03:15:04Z",
          "peerId": 22
        },
        {
          "asn": 20,
          "at": "2023-02-04T03:15:04Z",
          "peerId": 3,
          "peerIp": "10.11.12.3"
        },
        {
          "asn": 20,
          "at": "2023-02-04T03:15:04Z",
          "peerId": 4,
          "peerIp": "10.11.12.4"
        },
        {
          "asn": 20,
          "at": "2023-02-04T03:15:04Z",
          "peerId": 5,
          "peerIp": "10.11.12.5"
        },
        {
          "asn": 20,
          "at": "2023-02-04T03:15:04Z",
          "peerId": 7,
          "peerIp": "10.31.32.1"
        }
      ],
      "allViolationPeersCount": 10
    },
    "orgName": "AutomationOnly5",
    "policyId": "4d4816b9-e579-4209-a907-8d909aafa1f0",
    "policyName": "05 - Prefix Advertisement",
    "rule": "ALARM_RULE_PREFIX_ADVERTISEMENT",
    "severity": "ALARM_SEVERITY_RED",
    "state": "ALARM_STATE_ACTIVE",
    "tags": [
      "common tag",
      "prefix policy",
      "05 - Prefix Advertisement"
    ],
    "transitionedAt": "2023-02-04T03:16:25Z"
  }
  {
    "activatedAt": "2023-02-04T03:16:25Z",
    "alarmId": "ba974865-7e94-4623-ad8f-d660acf7d69f",
    "clearedAt": "2023-02-04T03:15:47Z",
    "expected": {
      "numPeersToClear": 1,
      "numPeersToTrigger": 2
    },
    "monitoredPrefix": "2002:da38:6400::/48",
```

```
"observed": {
  "allViolationPeers": [
    {
      "asn": 20,
      "at": "2023-02-04T03:15:04Z",
      "peerId": 23
    },
    {
      "asn": 20,
      "at": "2023-02-04T03:15:04Z",
      "peerId": 24
    },
    {
      "asn": 20,
      "at": "2023-02-04T03:15:04Z",
      "peerId": 25
    },
    {
      "asn": 20,
      "at": "2023-02-04T03:15:04Z",
      "peerId": 26
    },
    {
      "asn": 20,
      "at": "2023-02-04T03:15:04Z",
      "peerId": 27
    },
    {
      "asn": 20,
      "at": "2023-02-04T03:15:04Z",
      "peerId": 28
    },
    {
      "asn": 20,
      "at": "2023-02-04T03:15:04Z",
      "peerId": 29
    },
    {
      "asn": 20,
      "at": "2023-02-04T03:15:04Z",
      "peerId": 30
    },
    {
      "asn": 20,
      "at": "2023-02-04T03:15:04Z",
      "peerId": 31
    },
    {
      "asn": 20,
      "at": "2023-02-04T03:15:04Z",
      "peerId": 32
    },
    {
      "asn": 20,
      "at": "2023-02-04T03:15:04Z",
      "peerId": 6,
      "peerIp": "2000::20:100:10"
    },
    {
      "asn": 20,
      "at": "2023-02-04T03:15:04Z",
      "peerId": 8,
      "peerIp": "2000::30:100:10"
    }
```

```
    ],
    "allViolationPeersCount": 12
  },
  "orgName": "AutomationOnly5",
  "policyId": "4d4816b9-e579-4209-a907-8d909aafa1f0",
  "policyName": "05 - Prefix Advertisement",
  "rule": "ALARM_RULE_PREFIX_ADVERTISEMENT",
  "severity": "ALARM_SEVERITY_RED",
  "state": "ALARM_STATE_ACTIVE",
  "tags": [
    "common tag",
    "prefix policy",
    "05 - Prefix Advertisement"
  ],
  "transitionedAt": "2023-02-04T03:16:25Z"
}
```


Prefix Withdrawal Example

The following is an Amazon S3 notification and Google Storage notification log message example for a **Prefix Withdrawal** alarm.


```
{
  "activatedAt": "2023-02-04T03:20:36Z",
  "alarmId": "2e12713b-4ecf-4d59-868a-00f07aba47ae",
  "clearedAt": "2023-02-04T03:19:55Z",
  "expected": {
    "numPeersToClear": 1,
    "numPeersToTrigger": 2
  },
  "monitoredPrefix": "100.200.1.0/24",
  "observed": {
    "allViolationPeers": [
      {
        "at": "2023-02-04T03:19:13Z",
        "peerId": 1,
        "peerIp": "10.11.12.1"
      },
      {
        "at": "2023-02-04T03:19:13Z",
        "peerId": 19
      },
      {
        "at": "2023-02-04T03:19:13Z",
        "peerId": 20
      },
      {
        "at": "2023-02-04T03:19:13Z",
        "peerId": 21
      },
      {
        "at": "2023-02-04T03:19:13Z",
        "peerId": 22
      },
      {
        "at": "2023-02-04T03:19:13Z",
        "peerId": 3,
        "peerIp": "10.11.12.3"
      },
      {
        "at": "2023-02-04T03:19:13Z",
        "peerId": 4,
        "peerIp": "10.11.12.4"
      },
```

```
        {
          "at": "2023-02-04T03:19:13Z",
          "peerId": 5,
          "peerIp": "10.11.12.5"
        },
        {
          "at": "2023-02-04T03:19:13Z",
          "peerId": 7,
          "peerIp": "10.31.32.1"
        }
      ],
      "allViolationPeersCount": 9
    },
    "orgName": "AutomationOnly5",
    "policyId": "16105783-75c8-4c98-be71-b0a758645f41",
    "policyName": "06 - Prefix Withdrawal",
    "rule": "ALARM_RULE_PREFIX_WITHDRAWAL",
    "severity": "ALARM_SEVERITY_RED",
    "state": "ALARM_STATE_ACTIVE",
    "tags": [
      "common tag",
      "prefix policy",
      "06 - Prefix Withdrawal"
    ],
    "transitionedAt": "2023-02-04T03:20:36Z"
  }
  {
    "activatedAt": "2023-02-04T03:20:36Z",
    "alarmId": "3c4cf6e0-e6f2-475d-9030-4bc51a7e0550",
    "clearedAt": "2023-02-04T03:19:55Z",
    "expected": {
      "numPeersToClear": 1,
      "numPeersToTrigger": 2
    },
    "monitoredPrefix": "2002:64c8:100::/48",
    "observed": {
      "allViolationPeers": [
        {
          "at": "2023-02-04T03:19:13Z",
          "peerId": 23
        },
        {
          "at": "2023-02-04T03:19:13Z",
          "peerId": 24
        },
        {
          "at": "2023-02-04T03:19:13Z",
          "peerId": 25
        },
        {
          "at": "2023-02-04T03:19:13Z",
          "peerId": 26
        },
        {
          "at": "2023-02-04T03:19:13Z",
          "peerId": 27
        },
        {
          "at": "2023-02-04T03:19:13Z",
          "peerId": 28
        },
        {
          "at": "2023-02-04T03:19:13Z",
          "peerId": 29
```

```
      },
      {
        "at": "2023-02-04T03:19:13Z",
        "peerId": 30
      },
      {
        "at": "2023-02-04T03:19:13Z",
        "peerId": 31
      },
      {
        "at": "2023-02-04T03:19:13Z",
        "peerId": 32
      },
      {
        "at": "2023-02-04T03:19:13Z",
        "peerId": 6,
        "peerIp": "2000::20:100:10"
      },
      {
        "at": "2023-02-04T03:19:13Z",
        "peerId": 8,
        "peerIp": "2000::30:100:10"
      }
    ],
    "allViolationPeersCount": 12
  },
  "orgName": "AutomationOnly5",
  "policyId": "16105783-75c8-4c98-be71-b0a758645f41",
  "policyName": "06 - Prefix Withdrawal",
  "rule": "ALARM_RULE_PREFIX_WITHDRAWAL",
  "severity": "ALARM_SEVERITY_RED",
  "state": "ALARM_STATE_ACTIVE",
  "tags": [
    "common tag",
    "prefix policy",
    "06 - Prefix Withdrawal"
  ],
  "transitionedAt": "2023-02-04T03:20:36Z"
}
```


Prohibited IP Prefix Example

The following is an S3 and Google Storage notification log message example for a **Prohibited IP Prefix** (Full Bogon) alarm.


```
{
  "activatedAt": "2023-02-04T06:11:31Z",
  "alarmId": "a077c6cd-5a74-4378-8d60-e8acb39ae2c7",
  "clearedAt": "2023-02-04T06:09:26Z",
  "monitoredPeer": {
    "ciscoPeerIp": "104.236.154.30",
    "ciscoPeerName": "RS06",
    "peerIp": "10.11.12.5",
    "peerName": "FullBogon-1",
    "sessionId": "f5327ffb-221f-49d6-b8a2-2b812d02d35e"
  },
  "observed": {
    "lastViolationPeerPrefix": {
      "at": "2023-02-04T06:07:33Z",
      "bogonDetails": {
        "bogonType": "ALARM_BOGON_TYPE_FULL_BOGON",
        "prohibitedPrefixBlock": "5.44.248.0/21"
      },
      "prefix": "5.44.248.0/21"
```

```
    },
    "violationPrefixesCount": 1
  },
  "orgName": "AutomationOnly5",
  "policyId": "d011c5e4-54a1-41bb-8c7f-963d9caab208",
  "policyName": "19 - Prohibited IP Prefix - FullBogon",
  "rule": "ALARM_RULE_PROHIBITED_IP_PREFIX",
  "severity": "ALARM_SEVERITY_YELLOW",
  "state": "ALARM_STATE_ACTIVE",
  "transitionedAt": "2023-02-04T06:11:31Z"
}
{
  "activatedAt": "2023-02-04T06:11:31Z",
  "alarmId": "142659ed-15f1-4d60-b2d6-3d0da5c75b17",
  "clearedAt": "2023-02-04T06:09:26Z",
  "monitoredPeer": {
    "ciscoPeerIp": "2604:a880:1:20::2de:1001",
    "ciscoPeerName": "RS06",
    "peerIp": "2000::20:100:10",
    "peerName": "FullBogon-2",
    "sessionId": "639f069d-9ccd-46d0-b8b2-77054a199ce8"
  },
  "observed": {
    "lastViolationPeerPrefix": {
      "at": "2023-02-04T06:07:33Z",
      "bogonDetails": {
        "bogonType": "ALARM_BOGON_TYPE_FULL_BOGON",
        "prohibitedPrefixBlock": "2001:506:101::/48"
      },
      "prefix": "2001:506:101::/48"
    },
    "violationPrefixesCount": 1
  },
  "orgName": "AutomationOnly5",
  "policyId": "d011c5e4-54a1-41bb-8c7f-963d9caab208",
  "policyName": "19 - Prohibited IP Prefix - FullBogon",
  "rule": "ALARM_RULE_PROHIBITED_IP_PREFIX",
  "severity": "ALARM_SEVERITY_YELLOW",
  "state": "ALARM_STATE_ACTIVE",
  "transitionedAt": "2023-02-04T06:11:31Z"
}
```


ROA Expiry Example

The following is an Amazon S3 notification and Google Storage notification log message example for a **ROA Expiry** alarm.


```
{
  "activatedAt": "2023-02-04T03:27:02Z",
  "alarmId": "9f8eb76a-3eff-4e8b-809e-53bf0fd56ebe",
  "clearedAt": "2023-02-04T03:26:20Z",
  "expected": {
    "numPeersToTrigger": 1
  },
  "monitoredPrefix": "2002:101:7700::/48",
  "observed": {
    "allViolationPeers": [
      {
        "asn": 33,
        "at": "2023-02-04T03:25:38Z",
        "peerId": 23
      },
      {
        "asn": 33,
```

```
      "at": "2023-02-04T03:25:38Z",
      "peerId": 24
    },
    {
      "asn": 33,
      "at": "2023-02-04T03:25:38Z",
      "peerId": 25
    },
    {
      "asn": 33,
      "at": "2023-02-04T03:25:38Z",
      "peerId": 26
    },
    {
      "asn": 33,
      "at": "2023-02-04T03:25:38Z",
      "peerId": 27
    },
    {
      "asn": 33,
      "at": "2023-02-04T03:25:38Z",
      "peerId": 28
    },
    {
      "asn": 33,
      "at": "2023-02-04T03:25:38Z",
      "peerId": 29
    },
    {
      "asn": 33,
      "at": "2023-02-04T03:25:38Z",
      "peerId": 30
    },
    {
      "asn": 33,
      "at": "2023-02-04T03:25:38Z",
      "peerId": 31
    },
    {
      "asn": 33,
      "at": "2023-02-04T03:25:38Z",
      "peerId": 32
    },
    {
      "asn": 33,
      "at": "2023-02-04T03:25:38Z",
      "peerId": 6,
      "peerIp": "2000::20:100:10"
    },
    {
      "asn": 33,
      "at": "2023-02-04T03:25:38Z",
      "peerId": 8,
      "peerIp": "2000::30:100:10"
    }
  ],
  "allViolationPeersCount": 12,
  "roas": [
    {
      "asn": 33,
      "maxLength": 48,
      "notAfter": "2023-02-17T03:49:38Z",
      "notBefore": "2022-02-03T03:49:38Z",
      "prefix": "2002:101:7700::/48",
```

```
        "rpkiStatus": "ALARM_ROA_VALID",
        "trustAnchor": "ALARM_AFRINIC"
      },
      {
        "asn": 33,
        "maxLength": 48,
        "notAfter": "2023-02-17T19:24:49Z",
        "notBefore": "2022-02-03T19:24:49Z",
        "prefix": "2002:101:7700::/48",
        "rpkiStatus": "ALARM_ROA_VALID",
        "trustAnchor": "ALARM_AFRINIC"
      },
      {
        "asn": 33,
        "maxLength": 48,
        "notAfter": "2023-02-18T01:34:59Z",
        "notBefore": "2022-02-04T01:34:58Z",
        "prefix": "2002:101:7700::/48",
        "rpkiStatus": "ALARM_ROA_VALID",
        "trustAnchor": "ALARM_AFRINIC"
      }
    ]
  },
  "orgName": "AutomationOnly5",
  "policyId": "d3d47d8c-fee7-45ab-baee-3a860128aa65",
  "policyName": "08 - ROA Expiry",
  "rule": "ALARM_RULE_ROA_EXPIRY",
  "severity": "ALARM_SEVERITY_RED",
  "state": "ALARM_STATE_ACTIVE",
  "tags": [
    "common tag",
    "prefix policy",
    "08 - ROA Expiry"
  ],
  "transitionedAt": "2023-02-04T03:27:02Z"
}
{
  "activatedAt": "2023-02-04T03:27:02Z",
  "alarmId": "e85e68ad-e16d-4892-9fb9-c71bd92f9caf",
  "clearedAt": "2023-02-04T03:26:20Z",
  "expected": {
    "numPeersToTrigger": 1
  },
  "monitoredPrefix": "210.176.151.0/24",
  "observed": {
    "allViolationPeers": [
      {
        "asn": 33,
        "at": "2023-02-04T03:25:38Z",
        "peerId": 1,
        "peerIp": "10.11.12.1"
      },
      {
        "asn": 33,
        "at": "2023-02-04T03:25:38Z",
        "peerId": 19
      },
      {
        "asn": 33,
        "at": "2023-02-04T03:25:38Z",
        "peerId": 2,
        "peerIp": "10.11.12.2"
      },
      {
```

```
      "asn": 33,
      "at": "2023-02-04T03:25:38Z",
      "peerId": 20
    },
    {
      "asn": 33,
      "at": "2023-02-04T03:25:38Z",
      "peerId": 21
    },
    {
      "asn": 33,
      "at": "2023-02-04T03:25:38Z",
      "peerId": 22
    },
    {
      "asn": 33,
      "at": "2023-02-04T03:25:38Z",
      "peerId": 3,
      "peerIp": "10.11.12.3"
    },
    {
      "asn": 33,
      "at": "2023-02-04T03:25:38Z",
      "peerId": 4,
      "peerIp": "10.11.12.4"
    },
    {
      "asn": 33,
      "at": "2023-02-04T03:25:38Z",
      "peerId": 5,
      "peerIp": "10.11.12.5"
    },
    {
      "asn": 33,
      "at": "2023-02-04T03:25:38Z",
      "peerId": 7,
      "peerIp": "10.31.32.1"
    }
  ],
  "allViolationPeersCount": 10,
  "roas": [
    {
      "asn": 33,
      "maxLength": 24,
      "notAfter": "2023-02-17T03:49:38Z",
      "notBefore": "2022-02-03T03:49:38Z",
      "prefix": "210.176.151.0/24",
      "rpkiStatus": "ALARM_ROA_VALID",
      "trustAnchor": "ALARM_AFRINIC"
    },
    {
      "asn": 33,
      "maxLength": 24,
      "notAfter": "2023-02-17T19:24:49Z",
      "notBefore": "2022-02-03T19:24:49Z",
      "prefix": "210.176.151.0/24",
      "rpkiStatus": "ALARM_ROA_VALID",
      "trustAnchor": "ALARM_AFRINIC"
    },
    {
      "asn": 33,
      "maxLength": 24,
      "notAfter": "2023-02-18T01:34:58Z",
      "notBefore": "2022-02-04T01:34:58Z",
```

```
        "prefix": "210.176.151.0/24",
        "rpkiStatus": "ALARM_ROA_VALID",
        "trustAnchor": "ALARM_AFRINIC"
      }
    ]
  },
  "orgName": "AutomationOnly5",
  "policyId": "d3d47d8c-fee7-45ab-baee-3a860128aa65",
  "policyName": "08 - ROA Expiry",
  "rule": "ALARM_RULE_ROA_EXPIRY",
  "severity": "ALARM_SEVERITY_RED",
  "state": "ALARM_STATE_ACTIVE",
  "tags": [
    "common tag",
    "prefix policy",
    "08 - ROA Expiry"
  ],
  "transitionedAt": "2023-02-04T03:27:02Z"
}
```


ROA Not Found Example

The following is an Amazon S3 notification and Google Storage notification log message example for a **ROA Not Found** alarm.


```
{
  "activatedAt": "2023-02-04T03:22:07Z",
  "alarmId": "992266a8-bc34-4e6f-b396-6f0c956886ae",
  "monitoredPrefix": "2.2.2.2/32",
  "observed": {
    "allViolationPeers": [
      {
        "asn": 31,
        "at": "2023-02-04T01:34:58Z",
        "peerId": 1,
        "peerIp": "10.11.12.1"
      },
      {
        "asn": 31,
        "at": "2023-02-04T01:34:58Z",
        "peerId": 19
      },
      {
        "asn": 31,
        "at": "2023-02-04T01:34:58Z",
        "peerId": 2,
        "peerIp": "10.11.12.2"
      },
      {
        "asn": 31,
        "at": "2023-02-04T01:34:58Z",
        "peerId": 20
      },
      {
        "asn": 31,
        "at": "2023-02-04T01:34:58Z",
        "peerId": 21
      },
      {
        "asn": 31,
        "at": "2023-02-04T01:34:58Z",
        "peerId": 22
      },
      {
```

```
          "asn": 31,
          "at": "2023-02-04T01:34:58Z",
          "peerId": 3,
          "peerIp": "10.11.12.3"
        },
        {
          "asn": 31,
          "at": "2023-02-04T01:34:58Z",
          "peerId": 4,
          "peerIp": "10.11.12.4"
        },
        {
          "asn": 31,
          "at": "2023-02-04T01:34:58Z",
          "peerId": 5,
          "peerIp": "10.11.12.5"
        },
        {
          "asn": 31,
          "at": "2023-02-04T01:34:58Z",
          "peerId": 7,
          "peerIp": "10.31.32.1"
        }
      ],
      "allViolationPeersCount": 10
    },
    "orgName": "AutomationOnly5",
    "policyId": "588687b4-4e2c-44d6-8f93-56957139b4f4",
    "policyName": "07 - ROA Not Found",
    "rule": "ALARM_RULE_ROA_NOT_FOUND",
    "severity": "ALARM_SEVERITY_RED",
    "state": "ALARM_STATE_ACTIVE",
    "tags": [
      "common tag",
      "prefix policy",
      "07 - ROA Not Found"
    ],
    "transitionedAt": "2023-02-04T03:22:07Z"
  }
  {
    "activatedAt": "2023-02-04T03:22:07Z",
    "alarmId": "c7ff225d-f4e0-49d7-b607-f9d4f98b346f",
    "monitoredPrefix": "2002:202:202::/48",
    "observed": {
      "allViolationPeers": [
        {
          "asn": 31,
          "at": "2023-02-04T01:34:58Z",
          "peerId": 23
        },
        {
          "asn": 31,
          "at": "2023-02-04T01:34:58Z",
          "peerId": 24
        },
        {
          "asn": 31,
          "at": "2023-02-04T01:34:58Z",
          "peerId": 25
        },
        {
          "asn": 31,
          "at": "2023-02-04T01:34:58Z",
          "peerId": 26
```

```
        },
        {
          "asn": 31,
          "at": "2023-02-04T01:34:58Z",
          "peerId": 27
        },
        {
          "asn": 31,
          "at": "2023-02-04T01:34:58Z",
          "peerId": 28
        },
        {
          "asn": 31,
          "at": "2023-02-04T01:34:58Z",
          "peerId": 29
        },
        {
          "asn": 31,
          "at": "2023-02-04T01:34:58Z",
          "peerId": 30
        },
        {
          "asn": 31,
          "at": "2023-02-04T01:34:58Z",
          "peerId": 31
        },
        {
          "asn": 31,
          "at": "2023-02-04T01:34:58Z",
          "peerId": 32
        },
        {
          "asn": 31,
          "at": "2023-02-04T01:34:58Z",
          "peerId": 6,
          "peerIp": "2000::20:100:10"
        },
        {
          "asn": 31,
          "at": "2023-02-04T01:34:58Z",
          "peerId": 8,
          "peerIp": "2000::30:100:10"
        }
      ],
      "allViolationPeersCount": 12
    },
    "orgName": "AutomationOnly5",
    "policyId": "588687b4-4e2c-44d6-8f93-56957139b4f4",
    "policyName": "07 - ROA Not Found",
    "rule": "ALARM_RULE_ROA_NOT_FOUND",
    "severity": "ALARM_SEVERITY_RED",
    "state": "ALARM_STATE_ACTIVE",
    "tags": [
      "common tag",
      "prefix policy",
      "07 - ROA Not Found"
    ],
    "transitionedAt": "2023-02-04T03:22:07Z"
  }
```

ROA Failure Example

The following is an Amazon S3 notification and Google Storage notification log message example for an **ROA Failure** alarm.


```
{
  "activatedAt": "2023-02-04T03:31:32Z",
  "alarmId": "358c3f57-80b8-4685-baec-7d913f39988e",
  "clearedAt": "2023-02-04T03:30:51Z",
  "expected": {
    "numPeersToTrigger": 1,
    "originAsns": [
      24,
      1136
    ]
  },
  "monitoredPrefix": "194.45.8.0/22",
  "observed": {
    "allViolationPeers": [
      {
        "asn": 23,
        "at": "2023-02-04T03:30:09Z",
        "peerId": 1,
        "peerIp": "10.11.12.1"
      },
      {
        "asn": 23,
        "at": "2023-02-04T03:30:09Z",
        "peerId": 19
      },
      {
        "asn": 23,
        "at": "2023-02-04T03:30:09Z",
        "peerId": 2,
        "peerIp": "10.11.12.2"
      },
      {
        "asn": 23,
        "at": "2023-02-04T03:30:09Z",
        "peerId": 20
      },
      {
        "asn": 23,
        "at": "2023-02-04T03:30:09Z",
        "peerId": 21
      },
      {
        "asn": 23,
        "at": "2023-02-04T03:30:09Z",
        "peerId": 22
      },
      {
        "asn": 23,
        "at": "2023-02-04T03:30:09Z",
        "peerId": 3,
        "peerIp": "10.11.12.3"
      },
      {
        "asn": 23,
        "at": "2023-02-04T03:30:09Z",
        "peerId": 4,
        "peerIp": "10.11.12.4"
      },
      {
```

```
        "asn": 23,
        "at": "2023-02-04T03:30:09Z",
        "peerId": 5,
        "peerIp": "10.11.12.5"
      },
      {
        "asn": 23,
        "at": "2023-02-04T03:30:09Z",
        "peerId": 7,
        "peerIp": "10.31.32.1"
      }
    ],
    "allViolationPeersCount": 10
  },
  "orgName": "AutomationOnly5",
  "policyId": "0510e174-1553-4c12-ac9e-be68118c8bd2",
  "policyName": "09 - ROA Failure",
  "rule": "ALARM_RULE_ROA_FAILURE",
  "severity": "ALARM_SEVERITY_RED",
  "state": "ALARM_STATE_ACTIVE",
  "tags": [
    "common tag",
    "prefix policy",
    "09 - ROA Failure"
  ],
  "transitionedAt": "2023-02-04T03:31:32Z"
}
{
  "activatedAt": "2023-02-04T03:31:32Z",
  "alarmId": "4e0b7398-ae54-408e-95fc-e7bb17a7d952",
  "clearedAt": "2023-02-04T03:30:51Z",
  "expected": {
    "numPeersToTrigger": 1,
    "originAsns": [
      24
    ]
  },
  "monitoredPrefix": "2002:c22d:800::/48",
  "observed": {
    "allViolationPeers": [
      {
        "asn": 23,
        "at": "2023-02-04T03:30:09Z",
        "peerId": 23
      },
      {
        "asn": 23,
        "at": "2023-02-04T03:30:09Z",
        "peerId": 24
      },
      {
        "asn": 23,
        "at": "2023-02-04T03:30:09Z",
        "peerId": 25
      },
      {
        "asn": 23,
        "at": "2023-02-04T03:30:09Z",
        "peerId": 26
      },
      {
        "asn": 23,
        "at": "2023-02-04T03:30:09Z",
        "peerId": 27
```

```
      },
      {
        "asn": 23,
        "at": "2023-02-04T03:30:09Z",
        "peerId": 28
      },
      {
        "asn": 23,
        "at": "2023-02-04T03:30:09Z",
        "peerId": 29
      },
      {
        "asn": 23,
        "at": "2023-02-04T03:30:09Z",
        "peerId": 30
      },
      {
        "asn": 23,
        "at": "2023-02-04T03:30:09Z",
        "peerId": 31
      },
      {
        "asn": 23,
        "at": "2023-02-04T03:30:09Z",
        "peerId": 32
      },
      {
        "asn": 23,
        "at": "2023-02-04T03:30:09Z",
        "peerId": 6,
        "peerIp": "2000::20:100:10"
      },
      {
        "asn": 23,
        "at": "2023-02-04T03:30:09Z",
        "peerId": 8,
        "peerIp": "2000::30:100:10"
      }
    ],
    "allViolationPeersCount": 12
  },
  "orgName": "AutomationOnly5",
  "policyId": "0510e174-1553-4c12-ac9e-be68118c8bd2",
  "policyName": "09 - ROA Failure",
  "rule": "ALARM_RULE_ROA_FAILURE",
  "severity": "ALARM_SEVERITY_RED",
  "state": "ALARM_STATE_ACTIVE",
  "tags": [
    "common tag",
    "prefix policy",
    "09 - ROA Failure"
  ],
  "transitionedAt": "2023-02-04T03:31:32Z"
}
```


SubPrefix Advertisement Example

The following is an Amazon S3 notification and Google Storage log message example for a **SubPrefix Advertisement** alarm.


```
{
  "activatedAt": "2023-02-04T03:48:07Z",
  "alarmId": "4f90ba05-d16e-4cb1-8bfe-f9bb54fc96dd",
  "clearedAt": "2023-02-04T03:47:26Z",
```

```
"expected": {
  "numPeersToClear": 1,
  "numPeersToTrigger": 2,
  "originAsns": [
    754,
    755,
    1000,
    6000,
    6001,
    6002,
    6003,
    6004,
    6005,
    6006,
    6007,
    6008,
    6009,
    6010,
    6011,
    9541,
    9542,
    9543,
    12654,
    12655,
    28642,
    30175,
    45031,
    49622
  ],
  "originAsnsUsage": "ALARM_USAGE_IGNORE"
},
"monitoredPrefix": "2002:1764:100::/48",
"observed": {
  "allViolationPeers": [
    {
      "peerId": 28
    },
    {
      "peerId": 29
    }
  ],
  "allViolationPeersCount": 2,
  "lastViolationPeers": [
    {
      "asn": 6000,
      "at": "2023-02-04T03:45:01Z",
      "peerId": 28
    },
    {
      "asn": 6001,
      "at": "2023-02-04T03:45:02Z",
      "peerId": 29
    }
  ],
  "lastViolationPeersCount": 2,
  "lastViolationPrefix": "2002:1764:100::/49",
  "violationPrefixesCount": 10
},
"orgName": "AutomationOnly5",
"policyId": "634cc992-80f5-488e-bd42-bcb61217be9f",
"policyName": "12 - Subprefix Advertisement - Default",
"rule": "ALARM_RULE_SUBPREFIX_ADVERTISEMENT",
"severity": "ALARM_SEVERITY_GRAY",
"state": "ALARM_STATE_ACTIVE",
```

```
  "tags": [
    "common tag",
    "prefix policy",
    "12 - Subprefix Advertisement"
  ],
  "transitionedAt": "2023-02-04T03:48:07Z"
}
{
  "activatedAt": "2023-02-04T03:48:07Z",
  "alarmId": "6e1e50ff-e57f-4a2b-9814-7c5a71b01b1d",
  "clearedAt": "2023-02-04T03:47:26Z",
  "expected": {
    "numPeersToClear": 1,
    "numPeersToTrigger": 2,
    "originAsns": [
      754,
      755,
      1000,
      6000,
      6001,
      6002,
      6003,
      6004,
      6005,
      6006,
      6007,
      6008,
      6009,
      6010,
      6011,
      9541,
      9542,
      9543,
      12654,
      12655,
      28642,
      30175,
      45031,
      49622
    ],
    "originAsnsUsage": "ALARM_USAGE_IGNORE"
  },
  "monitoredPrefix": "23.100.1.0/24",
  "observed": {
    "allViolationPeers": [
      {
        "peerId": 1
      },
      {
        "peerId": 19
      }
    ],
    "allViolationPeersCount": 2,
    "lastViolationPeers": [
      {
        "asn": 6000,
        "at": "2023-02-04T03:45:01Z",
        "peerId": 1,
        "peerIp": "10.11.12.1"
      },
      {
        "asn": 6001,
        "at": "2023-02-04T03:45:01Z",
        "peerId": 19
```

```
      }
    ],
    "lastViolationPeersCount": 2,
    "lastViolationPrefix": "23.100.1.0/25",
    "violationPrefixesCount": 8
  },
  "orgName": "AutomationOnly5",
  "policyId": "634cc992-80f5-488e-bd42-bcb61217be9f",
  "policyName": "12 - Subprefix Advertisement - Default",
  "rule": "ALARM_RULE_SUBPREFIX_ADVERTISEMENT",
  "severity": "ALARM_SEVERITY_GRAY",
  "state": "ALARM_STATE_ACTIVE",
  "tags": [
    "common tag",
    "prefix policy",
    "12 - Subprefix Advertisement"
  ],
  "transitionedAt": "2023-02-04T03:48:07Z"
}
```


Unexpected AS Prefix Example

The following is an Amazon S3 notification and Google Storage notification log message example for an **Unexpected AS Prefix** alarm.


```
{
  "activatedAt": "2023-02-04T02:58:11Z",
  "alarmId": "6a6be977-ecf3-423c-bf4e-fc9118659a69",
  "clearedAt": "2023-02-04T02:57:43Z",
  "expected": {
    "numPeersToClear": 1,
    "numPeersToTrigger": 2
  },
  "monitoredAsn": 601,
  "observed": {
    "allViolationPeers": [
      {
        "peerId": 1
      },
      {
        "peerId": 2
      },
      {
        "peerId": 3
      },
      {
        "peerId": 4
      },
      {
        "peerId": 5
      },
      {
        "peerId": 7
      },
      {
        "peerId": 19
      },
      {
        "peerId": 20
      },
      {
        "peerId": 21
      },
      {
```

```
      "peerId": 22
    }
  ],
  "allViolationPeersCount": 10,
  "lastViolationPeers": [
    {
      "asn": 601,
      "at": "2023-02-04T02:55:11Z",
      "peerId": 1,
      "peerIp": "10.11.12.1"
    },
    {
      "asn": 601,
      "at": "2023-02-04T02:55:11Z",
      "peerId": 19
    },
    {
      "asn": 601,
      "at": "2023-02-04T02:55:11Z",
      "peerId": 2,
      "peerIp": "10.11.12.2"
    },
    {
      "asn": 601,
      "at": "2023-02-04T02:55:11Z",
      "peerId": 20
    },
    {
      "asn": 601,
      "at": "2023-02-04T02:55:11Z",
      "peerId": 21
    },
    {
      "asn": 601,
      "at": "2023-02-04T02:55:11Z",
      "peerId": 22
    },
    {
      "asn": 601,
      "at": "2023-02-04T02:55:11Z",
      "peerId": 3,
      "peerIp": "10.11.12.3"
    },
    {
      "asn": 601,
      "at": "2023-02-04T02:55:11Z",
      "peerId": 4,
      "peerIp": "10.11.12.4"
    },
    {
      "asn": 601,
      "at": "2023-02-04T02:55:11Z",
      "peerId": 5,
      "peerIp": "10.11.12.5"
    },
    {
      "asn": 601,
      "at": "2023-02-04T02:55:11Z",
      "peerId": 7,
      "peerIp": "10.31.32.1"
    }
  ],
  "lastViolationPeersCount": 10,
  "lastViolationPrefix": "101.1.1.0/24",
```

```
    "violationPrefixesCount": 1
  },
  "orgName": "AutomationOnly5",
  "policyId": "5e3288f9-6e6d-4df7-a862-b638e2d17b9f",
  "policyName": "01 - Unexpected AS Prefix",
  "rule": "ALARM_RULE_UNEXPECTED_AS_PREFIX",
  "severity": "ALARM_SEVERITY_RED",
  "state": "ALARM_STATE_ACTIVE",
  "tags": [
    "common tag",
    "asn policy",
    "01 - Unexpected AS Prefix"
  ],
  "transitionedAt": "2023-02-04T02:58:11Z"
}
```


Upstream AS Change Example

The following is an Amazon S3 notification and Google Storage notification log message example for an **Upstream AS Change** alarm.


```
{
  "activatedAt": "2023-02-04T03:36:49Z",
  "alarmId": "82f76592-14ca-42ef-b446-149c1d4be731",
  "clearedAt": "2023-02-04T03:36:09Z",
  "expected": {
    "numPeersToClear": 1,
    "numPeersToTrigger": 2,
    "upstreamAsns": [
      12345
    ]
  },
  "monitoredPrefix": "2002:ab64:1100::/48",
  "observed": {
    "allViolationPeers": [
      {
        "asn": 6504,
        "at": "2023-02-04T03:33:54Z",
        "peerId": 6,
        "peerIp": "2000::20:100:10"
      },
      {
        "asn": 6503,
        "at": "2023-02-04T03:33:54Z",
        "peerId": 23
      },
      {
        "asn": 6508,
        "at": "2023-02-04T03:33:54Z",
        "peerId": 27
      },
      {
        "asn": 6502,
        "at": "2023-02-04T03:33:54Z",
        "peerId": 8,
        "peerIp": "2000::30:100:10"
      },
      {
        "asn": 6509,
        "at": "2023-02-04T03:33:54Z",
        "peerId": 28
      },
      {
        "asn": 6505,
```

```
        "at": "2023-02-04T03:33:54Z",
        "peerId": 24
      },
      {
        "asn": 6510,
        "at": "2023-02-04T03:33:54Z",
        "peerId": 29
      },
      {
        "asn": 6507,
        "at": "2023-02-04T03:33:54Z",
        "peerId": 26
      },
      {
        "asn": 6512,
        "at": "2023-02-04T03:33:54Z",
        "peerId": 31
      },
      {
        "asn": 6513,
        "at": "2023-02-04T03:33:54Z",
        "peerId": 32
      },
      {
        "asn": 6506,
        "at": "2023-02-04T03:33:54Z",
        "peerId": 25
      },
      {
        "asn": 6511,
        "at": "2023-02-04T03:33:54Z",
        "peerId": 30
      }
    ],
    "allViolationPeersCount": 12
  },
  "orgName": "AutomationOnly5",
  "policyId": "c37b83be-0213-4bb2-b391-7f02b3cec061",
  "policyName": "10 - Upstream AS Change",
  "rule": "ALARM_RULE_UPSTREAM_AS_CHANGE",
  "severity": "ALARM_SEVERITY_RED",
  "state": "ALARM_STATE_ACTIVE",
  "tags": [
    "common tag",
    "prefix policy",
    "10 - Upstream AS Change"
  ],
  "transitionedAt": "2023-02-04T03:36:49Z"
}
{
  "activatedAt": "2023-02-04T03:36:49Z",
  "alarmId": "a778b4be-e23f-42d8-8880-5402f59c1495",
  "clearedAt": "2023-02-04T03:36:09Z",
  "expected": {
    "numPeersToClear": 1,
    "numPeersToTrigger": 2,
    "upstreamAsns": [
      12345
    ]
  },
  "monitoredPrefix": "171.100.17.0/24",
  "observed": {
    "allViolationPeers": [
      {
```

```
        "asn": 6505,
        "at": "2023-02-04T03:33:54Z",
        "peerId": 3,
        "peerIp": "10.11.12.3"
      },
      {
        "asn": 6503,
        "at": "2023-02-04T03:33:54Z",
        "peerId": 5,
        "peerIp": "10.11.12.5"
      },
      {
        "asn": 6504,
        "at": "2023-02-04T03:33:54Z",
        "peerId": 4,
        "peerIp": "10.11.12.4"
      },
      {
        "asn": 6509,
        "at": "2023-02-04T03:33:54Z",
        "peerId": 20
      },
      {
        "asn": 6508,
        "at": "2023-02-04T03:33:54Z",
        "peerId": 19
      },
      {
        "asn": 6507,
        "at": "2023-02-04T03:33:54Z",
        "peerId": 1,
        "peerIp": "10.11.12.1"
      },
      {
        "asn": 6511,
        "at": "2023-02-04T03:33:54Z",
        "peerId": 22
      },
      {
        "asn": 6502,
        "at": "2023-02-04T03:33:54Z",
        "peerId": 7,
        "peerIp": "10.31.32.1"
      },
      {
        "asn": 6510,
        "at": "2023-02-04T03:33:54Z",
        "peerId": 21
      },
      {
        "asn": 6506,
        "at": "2023-02-04T03:33:54Z",
        "peerId": 2,
        "peerIp": "10.11.12.2"
      }
    ],
    "allViolationPeersCount": 10
  },
  "orgName": "AutomationOnly5",
  "policyId": "c37b83be-0213-4bb2-b391-7f02b3cec061",
  "policyName": "10 - Upstream AS Change",
  "rule": "ALARM_RULE_UPSTREAM_AS_CHANGE",
  "severity": "ALARM_SEVERITY_RED",
  "state": "ALARM_STATE_ACTIVE",
```

```
  "tags": [
    "common tag",
    "prefix policy",
    "10 - Upstream AS Change"
  ],
  "transitionedAt": "2023-02-04T03:36:49Z"
}
```


Valid AS Path Example

The following is an Amazon S3 notification and Google Storage notification log message example for a **Valid AS Path** alarm.

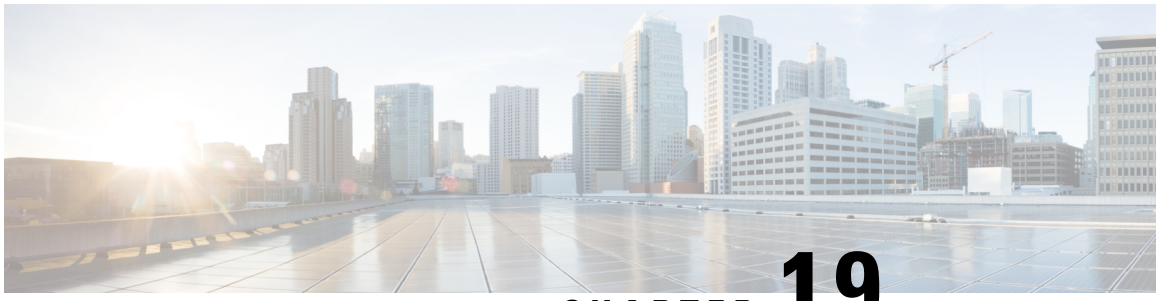

```
{
  "activatedAt": "2023-02-04T03:42:08Z",
  "alarmId": "7cc0e8d0-cef5-422f-a9b9-e6dd227e2bfc",
  "clearedAt": "2023-02-04T03:41:08Z",
  "expected": {
    "numPeersToClear": 1,
    "numPeersToTrigger": 2,
    "validAsPathPattern": "108 (999|400) 705"
  },
  "monitoredPrefix": "2002:dc45:500::/48",
  "observed": {
    "allViolationPeers": [
      {
        "asPath": [
          108,
          500,
          755
        ],
        "asn": 755,
        "at": "2023-02-04T03:39:27Z",
        "peerId": 23
      },
      {
        "asPath": [
          108,
          500,
          755
        ],
        "asn": 755,
        "at": "2023-02-04T03:39:27Z",
        "peerId": 24
      },
      {
        "asPath": [
          108,
          500,
          755
        ],
        "asn": 755,
        "at": "2023-02-04T03:39:27Z",
        "peerId": 25
      },
      {
        "asPath": [
          108,
          500,
          755
        ],
        "asn": 755,
        "at": "2023-02-04T03:39:27Z",
        "peerId": 26
```

```
},
{
  "asPath": [
    108,
    500,
    755
  ],
  "asn": 755,
  "at": "2023-02-04T03:39:27Z",
  "peerId": 27
},
{
  "asPath": [
    108,
    500,
    755
  ],
  "asn": 755,
  "at": "2023-02-04T03:39:27Z",
  "peerId": 28
},
{
  "asPath": [
    108,
    500,
    755
  ],
  "asn": 755,
  "at": "2023-02-04T03:39:27Z",
  "peerId": 29
},
{
  "asPath": [
    108,
    500,
    755
  ],
  "asn": 755,
  "at": "2023-02-04T03:39:27Z",
  "peerId": 30
},
{
  "asPath": [
    108,
    500,
    755
  ],
  "asn": 755,
  "at": "2023-02-04T03:39:27Z",
  "peerId": 31
},
{
  "asPath": [
    108,
    500,
    755
  ],
  "asn": 755,
  "at": "2023-02-04T03:39:27Z",
  "peerId": 32
},
{
  "asPath": [
    108,
```

```
            500,
            755
          ],
          "asn": 755,
          "at": "2023-02-04T03:39:27Z",
          "peerId": 6,
          "peerIp": "2000::20:100:10"
        },
        {
          "asPath": [
            108,
            500,
            755
          ],
          "asn": 755,
          "at": "2023-02-04T03:39:27Z",
          "peerId": 8,
          "peerIp": "2000::30:100:10"
        }
      ],
      "allViolationPeersCount": 12
    },
    "orgName": "AutomationOnly5",
    "policyId": "1b1d7a95-1104-4434-8f72-33ba216a7e7f",
    "policyName": "11 - Valid AS Path",
    "rule": "ALARM_RULE_VALID_AS_PATH_VIOLATION",
    "severity": "ALARM_SEVERITY_YELLOW",
    "state": "ALARM_STATE_ACTIVE",
    "tags": [
      "common tag",
      "prefix policy",
      "11 - Valid AS Path"
    ],
    "transitionedAt": "2023-02-04T03:42:08Z"
  }
  {
    "activatedAt": "2023-02-04T03:42:08Z",
    "alarmId": "86304e9c-50ce-4ec2-89a2-2c84ab10658b",
    "clearedAt": "2023-02-04T03:41:08Z",
    "expected": {
      "numPeersToClear": 1,
      "numPeersToTrigger": 2,
      "validAsPathPattern": "108 (999|400) 705"
    },
    "monitoredPrefix": "220.69.5.0/24",
    "observed": {
      "allViolationPeers": [
        {
          "asPath": [
            108,
            500,
            755
          ],
          "asn": 755,
          "at": "2023-02-04T03:39:27Z",
          "peerId": 1,
          "peerIp": "10.11.12.1"
        },
        {
          "asPath": [
            108,
            500,
            755
          ],
```

```
  "asn": 755,
  "at": "2023-02-04T03:39:27Z",
  "peerId": 19
},
{
  "asPath": [
    108,
    500,
    755
  ],
  "asn": 755,
  "at": "2023-02-04T03:39:27Z",
  "peerId": 2,
  "peerIp": "10.11.12.2"
},
{
  "asPath": [
    108,
    500,
    755
  ],
  "asn": 755,
  "at": "2023-02-04T03:39:27Z",
  "peerId": 20
},
{
  "asPath": [
    108,
    500,
    755
  ],
  "asn": 755,
  "at": "2023-02-04T03:39:27Z",
  "peerId": 21
},
{
  "asPath": [
    108,
    500,
    755
  ],
  "asn": 755,
  "at": "2023-02-04T03:39:27Z",
  "peerId": 22
},
{
  "asPath": [
    108,
    500,
    755
  ],
  "asn": 755,
  "at": "2023-02-04T03:39:27Z",
  "peerId": 3,
  "peerIp": "10.11.12.3"
},
{
  "asPath": [
    108,
    500,
    755
  ],
  "asn": 755,
  "at": "2023-02-04T03:39:27Z",
```

```
        "peerId": 4,
        "peerIp": "10.11.12.4"
      },
      {
        "asPath": [
          108,
          500,
          755
        ],
        "asn": 755,
        "at": "2023-02-04T03:39:27Z",
        "peerId": 5,
        "peerIp": "10.11.12.5"
      },
      {
        "asPath": [
          108,
          500,
          755
        ],
        "asn": 755,
        "at": "2023-02-04T03:39:27Z",
        "peerId": 7,
        "peerIp": "10.31.32.1"
      }
    ],
    "allViolationPeersCount": 10
  },
  "orgName": "AutomationOnly5",
  "policyId": "1b1d7a95-1104-4434-8f72-33ba216a7e7f",
  "policyName": "11 - Valid AS Path",
  "rule": "ALARM_RULE_VALID_AS_PATH_VIOLATION",
  "severity": "ALARM_SEVERITY_YELLOW",
  "state": "ALARM_STATE_ACTIVE",
  "tags": [
    "common tag",
    "prefix policy",
    "11 - Valid AS Path"
  ],
  "transitionedAt": "2023-02-04T03:42:08Z"
}
```



CHAPTER 19

Configure Devices

Add Devices to Crosswork Traffic Analysis

To add devices to Crosswork Traffic Analysis:

Before you begin

Confirm that there is an active data gateway in Crosswork Cloud. For more information, see Get Started with Crosswork Cloud Traffic Analysis.

Step 1 Configure BGP, SNMP, and network flow monitoring protocols on the devices.

Step 2 Add device credentials for BGP, SSH (optional), and SNMP to be used when adding devices.

Step 3 Add or import devices.

Step 4 Designate an External Interface

What to do next

- View and create policies to define what normal traffic should look like and notify you when they don't.

Add Devices to Crosswork Trust Insights

To add devices to Crosswork Trust Insights:

Before you begin

Confirm that there is an active data gateway in Crosswork Cloud. For more information, see Get Started with Crosswork Cloud Trust Insights.

Step 1 Confirm that the Cisco IOS XR version on your devices are supported.
Step 2 Verify Router Configuration
Step 3 Configure Limited Privilege User
Step 4 Add device credential profiles to be used when adding devices.
Step 5 Add or import devices.
Step 6 Initiate a dossier collection to get the latest device information.

Prerequisites for Adding Devices for Traffic Analysis

Before you add devices to Traffic Analysis, ensure that your devices have SSH and the following protocols configured:

Table 24: Protocol Configurations

Protocol	Example
SNMP	SNMP Configuration Examples, on page 153
BGP	BGP Configuration Example for Cisco IOS Devices, on page 153
Network Flow Monitoring	• Netflow Configuration Example for Cisco IOS XR Devices, on page 155 • IPFIX Configuration Example for Cisco IOS XR Devices, on page 156

If your devices are configured to restrict certain commands, you must ensure the following CLI commands are allowed:

- `show platform security integrity dossier`
- `show version`

The following sections contain configuration examples.

SNMP Configuration Examples

The following code shows examples of SNMP configurations.

- SNMPv2 configuration example:

```
snmp-server community flow123 RO
```

  In the previous example, **flow123** should match the configuration from the SNMP communities.

- SNMPv3 configuration examples:
  - For SNMPv3 without authentication and without privacy:

```
snmp-server group [groupname] v3 noauth
snmp-server user [username] [groupname] v3
```

  - For SNMPv3 with authentication and without privacy:

```
snmp-server group [groupname] v3 auth
snmp-server user [username] [groupname] auth [md5|sha] <auth-password>
```

  - For SNMPv3 with authentication and privacy:

```
snmp-server group [groupname] v3 priv
snmp-server user [username] [groupname] auth [md5|sha] <auth-password> priv [aes
128] <priv-password>
```

  Crosswork Cloud Traffic Analysis supports SNMPv3 128-bit only for the privacy protocol.

- (Optional) You can use the **snmp-server view** command to restrict SNMPv3 access. The following command examples show SNMP object identifiers (OIDs) read by Crosswork Cloud Traffic Analysis:

```
snmp-server view [view_name] 1.3.6.1.2.1.1 included
snmp-server view [view_name] 1.3.6.1.2.1.2 included
snmp-server view [view_name] 1.3.6.1.2.1.31 included

snmp-server group [groupname] v3 [noauth|auth|priv] read [view_name]
```

BGP Configuration Example for Cisco IOS Devices

The following code is an example of a BGP configuration for Cisco IOS devices:

Note All BGP prefixes must be shared with Cisco Crosswork Data Gateway.

Cisco IOS XE

```
router bgp <asn> << This must match the ASN in the CDG DEVICE configuration page in the
Crosswork Cloud UI
>>
bgp router-id <router-id>
bgp log-neighbor-changes
no bgp default ipv4-unicast
neighbor <CDG-ipv4-address> remote-as <CDG-asn>  << This must match the ASN of the CDG in
the Crosswork Cloud UI. It should be a Private ASN number. >>
neighbor <CDG-ipv4-address> description Cisco CrossWork Cloud CDG IPv4
neighbor <CDG-ipv4-address> ebgp-multihop 255
neighbor <CDG-ipv4-address> update-source <src-interface>
!
```

```
neighbor <CDG-ipv6-address> remote-as <CDG-asn>   << This must match the ASN of the CDG in
 the Crosswork Cloud UI. It should be a Private ASN number. >>
neighbor <CDG-ipv6-address> description Cisco CrossWork Cloud CDG IPv6
neighbor <CDG-ipv6-address> ebgp-multihop 255
neighbor <CDG-ipv6-address> update-source <src-interface>
!
address-family ipv4
  neighbor <CDG-ipv4-address> activate
  neighbor <CDG-ipv4-address> send-community both
  neighbor <CDG-ipv4-address> filter-list 2 in
  neighbor <CDG-ipv4-address> filter-list 1 out
exit-address-family
!
address-family ipv6
  neighbor <CDG-ipv6-address> activate
  neighbor <CDG-ipv6-address> send-community both
  neighbor <CDG-ipv6-address> filter-list 2 in
  neighbor <CDG-ipv6-address> filter-list 1 out
exit-address-family
!
ip as-path access-list 1 permit .*   <<All BGP prefixes from the device must be shared with
 Cisco CrossWork Cloud CDG>>
ip as-path access-list 2 deny .*
!
```

Cisco IOS XR

```
router bgp <asn> << This must match the ASN in the CDG DEVICE configuration page in the
Crosswork Cloud UI
>>
 bgp router-id <router-id>
 address-family ipv4 unicast
 !
 address-family ipv6 unicast
 !
 neighbor <CDG-ipv4-address>
  remote-as <CDG-asn>    << This must match the ASN of the CDG in the Crosswork Cloud UI.
It should be a Private ASN number. >>

  ebgp-multihop 255
  description Cisco CrossWork Cloud CDG IPv4
  update-source <src-interface>
  address-family ipv4 unicast
   route-policy DROP in
   route-policy PASS out
 !
 neighbor <route-server-ipv6>
  remote-as <CDG-asn>   << This must match the ASN of the CDG in the Crosswork Cloud UI.
It should be a Private ASN number. >>

  ebgp-multihop 255
  description Cisco CrossWork Route Server IPv6
  update-source <src-interface>
  address-family ipv6 unicast
   route-policy DROP in
   route-policy PASS out
!
route-policy PASS
 pass
end-policy
!
route-policy DROP
 drop
end-policy
```

```
!
```

where

- `<asn>` is the BGP AS number in your network
- `<router-id>` is the BPG router ID in your network
- `<CDG-asn>` is the BGP ASN number of CDG. It should be a Private ASN number
- `<src-interface>` is the BGP source interface in your network
- `<CDG-ipv4-address>` is the IPv4 address of CDG
- `<CDG-ipv6-address>` is the IPv6 address of CDG

Netflow Configuration Example for Cisco IOS XR Devices

The following code shows Netflow configuration examples for Cisco IOS XR devices:

IPv4 Example:

```
flow exporter-map ccni
 packet-length 1468
 version v9
  options sampler-table timeout 15
  template data timeout 15
  template options timeout 15
 !
 transport udp 2055
 source GigabitEthernet0/0/0/0
 destination 172.24.96.171  << this is the IP address of the CDG >>
!
flow monitor-map ccni
 record ipv4
 exporter ccni
 cache entries 1000000
 cache timeout active 12
 cache timeout update 15
!
sampler-map ccni-sampler
 random 1 out-of 1000
!
interface GigabitEthernet0/0/0/0
 ipv4 address 172.24.96.141 255.255.255.128
 flow ipv4 monitor ccni sampler ccni-sampler ingress
```

Example for exporting NetFlow IPv6 records through an IPv4 connection:

Note In this example, 192.0.2.169 is the IPv4 address of the Crosswork Data Gateway.

```
flow exporter-map ccni
 packet-length 1468
 version v9
  options sampler-table timeout 15
  template data timeout 15
  template options timeout 15
 !
 transport udp 2055
```

```
 source GigabitEthernet0/0/0/0
 destination 192.0.2.169  << this is the IP address of the CDG >>
!
flow monitor-map ccni-ipv6
 record ipv6
 exporter ccni
 cache entries 1000000
 cache timeout active 12
 cache timeout update 15
!
sampler-map ccni-sampler
random 1 out-of 1000
!
interface GigabitEthernet0/0/0/0
 ipv6 address 2001:100:100::1/64
flow ipv6 monitor ccni-ipv6 sampler ccni-sampler ingress
```

Applying IPv4 and IPv6 Example:

```
flow exporter-map ccni
packet-length 1468
version v9
  options sampler-table timeout 15
  template data timeout 15
  template options timeout 15
!
transport udp 2055
source GigabitEthernet 0/0/0/0
destination 172.24.96.171 << this is the IP address of the CDG >>
!
flow monitor-map ccni
  record ipv4
  exporter ccni
  cache entries 1000000
  cache timeout active 12
  cache timeout update 15
!
flow monitor-map ccni-ipv6
  record ipv6
  exporter ccni
  cache entries 1000000
  cache timeout active 12
  cache timeout update 15

sampler-map ccni-sampler
  random 1 out-of 1000
!
interface GigabitEthernet0/0/0/0

  ipv4 address 172.24.96.141 255.255.255.128
  ipv6 address 2001:100:100::1/64
  flow ipv4 monitor ccni sampler ccni-sampler ingress
  flow ipv6 monitor ccni-ipv6 sampler ccni-sampler ingress
```

IPFIX Configuration Example for Cisco IOS XR Devices

The following code shows an IPFIX configuration example for Cisco IOS XR devices:

```
flow exporter-map ccni
 packet-length 1468
 version ipfix
  options sampler-table timeout 15
  template data timeout 15
  template options timeout 15
 !
 transport udp 2055
 source GigabitEthernet0/0/0/0
 destination 172.24.96.184
!
flow monitor-map ccni
 record ipv4
 exporter ccni
 cache entries 1000000
 cache timeout active 3
 cache timeout update 3
!
sampler-map ccni-sampler
 random 1 out-of 1000
!
interface TenGigE0/0/0/16
 description internal interface
 ipv4 address 182.1.0.1 255.255.255.0
 flow ipv4 monitor ccni sampler ccni-sampler ingress
!
interface TenGigE0/0/0/27
 description external interface
 ipv4 address 184.1.0.1 255.255.255.0
 flow ipv4 monitor ccni sampler ccni-sampler ingress
```

SNMP Object Identifiers Used by Traffic Analysis

If you want to create a specific SNMP view for Crosswork Cloud Traffic Analysis, the following list contains the SNMP object identifiers (OIDs) that Crosswork Cloud Traffic Analysis uses.

- sysDescr—1.3.6.1.2.1.1.1.0
- sysObjectID—1.3.6.1.2.1.1.2.0
- sysUpTime—1.3.6.1.2.1.1.3.0
- sysName—1.3.6.1.2.1.1.5.0
- sysLocation—1.3.6.1.2.1.1.6.0
- ifDescr—1.3.6.1.2.1.2.2.1.2
- ifType—1.3.6.1.2.1.2.2.1.3
- ifSpeed—1.3.6.1.2.1.2.2.1.5
- ifOperStatus—1.3.6.1.2.1.2.2.1.8
- ifName—1.3.6.1.2.1.31.1.1.1.1
- ifHCSpeed—1.3.6.1.2.1.31.1.1.1.15
- ifHCInOctets—1.3.6.1.2.1.31.1.1.1.6
- ifHCOutOctets—1.3.6.1.2.1.31.1.1.1.10

Configure Interfaces

Designate an External Interface for Crosswork Traffic Analysis

After you add devices, you need to verify their SNMP status and then configure one or more interfaces to be *external* interfaces.Crosswork Cloud Traffic Analysis cannot display traffic data until you designate an external interface.

Step 1 In the main window, click **Configure** > **Devices**.

Step 2 Click on a device name in the **Device** column.

Step 3 Hover your cursor over SNMP, which appears between Crosswork Data Gateway and Devices, and ensure that the status is **Connected**.

By default, all interfaces are designated as *internal* interfaces. You need to select the external interface on your device and designate it as *external*.

Step 4 Click the **Traffic Analysis** tab, then click **Interfaces**.

Step 5 Select one or more external interfaces, then click **Set External**.

Crosswork Cloud Traffic Analysis recognizes the interface as an external interface.

Assign a Committed Information Rate (CIR) to an Interface

The Committed Information Rate (CIR) allows you to specify the bandwidth allowed on an interface if it is less than the physical capacity of that interface. It is useful to specify this, so that all calculations for interface capacity utilization refer to the permitted capacity rather than the physical capacity. For example, a 10 Gbps interface may only support a CIR of 1 Gbps. To accurately get an understanding of interface utilization in your network, you may want to base capacity calculations on the CIR of an interface. To assign a CIR to an interface:

Step 1 In the main window, click > **Interfaces**.

Step 2 From the **Interfaces** column, click on an interface name.

Step 3 Click **Edit**.

Step 4 In the **Interface Capacity Override** area, you can see what the interface capacity is currently set at. Toggle the switch to **ENABLED**.

Step 5 Enter the CIR for this interface. It must be lower than the physical interface capacity, but not less than 10 Mbps.

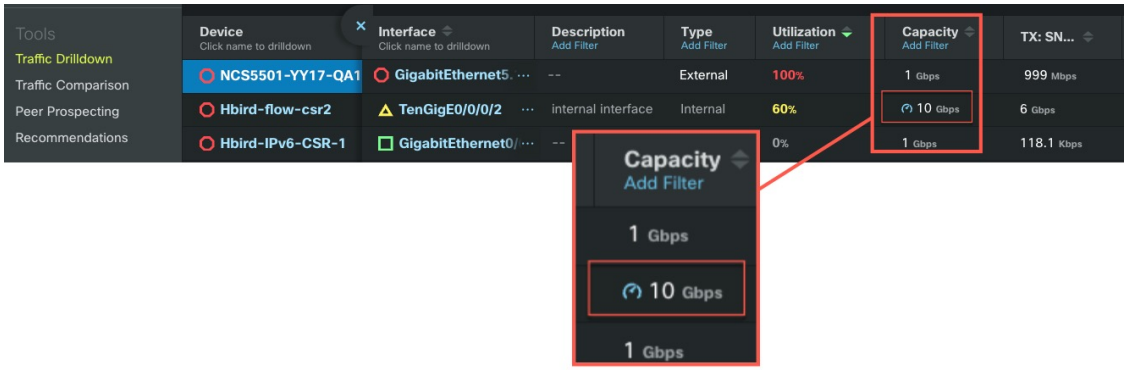
Step 6 Click **Save**.

After a CIR is assigned, all capacity calculations are based on the CIR. This means that interface utilization thresholds set in policies, as well as all interface capacity values displayed in Crosswork Traffic Analysis, use the CIRs assigned to the applicable interfaces.

Identify CIR Interfaces

All interface capacity values that have an assigned CIR displays a CIR icon ( ). For example:

Figure 4: Traffic Drilldown Example



Prerequisites for Adding Devices to Crosswork Trust Insights

Before you add your Cisco IOS XR routers to Crosswork Cloud Trust Insights, you must ensure the following router settings:

- Ensure your devices have the necessary supported image of IOS XR. See the Cisco Crosswork Cloud Release Notes for supported images.
- Verify that enrollment keys and certificates are properly generated within IOS XR. See Verify Router Configuration for Crosswork Trust Insights, on page 159 for more information.
- Ensure you configure a limited privilege user. See Configure Limited Privilege User for Crosswork Trust Insights, on page 163 for more information.

Verify Router Configuration for Crosswork Trust Insights

Before you use Crosswork Cloud Trust Insights, you need to verify that your Cisco IOS XR routers are configured correctly to allow their trust information to be accessed. Follow these steps to ensure your routers are configured correctly for Crosswork Cloud Trust Insights.

Note The following example is the minimal Cisco IOS XR configuration required to enable Crosswork Cloud Trust Insights. For more configuration examples, refer to the configuration guide that corresponds to the platform on which you want to enable Crosswork Cloud Trust Insights. See Related Hardware Documentation for direct links to the configuration guides.

Step 1 Log into your router and enter the following command:

```
ios# show running-config
```

Step 2 Verify that the output contains the following configuration elements:

- Hostname
- DNS domain name
- SSH server enabled
- Netconf-yang enabled for SSH
- Valid IP interface configured and reachable for inbound SSH access
- Appropriate static default route configured

The following example output shows what you should see:

```
hostname xr9kv-001
domain name test.cisco.com
!
netconf-yang agent
 ssh
!
interface MgmtEth0/RP0/CPU0/0
 ipv4 address 192.168.1.123 255.255.255.0
!
router static
 address-family ipv4 unicast
  0.0.0.0/0 192.168.1.1
  !
!
ssh server v2
ssh server netconf vrf default
```

Step 3 Ensure the router can be reached by SSH.

Step 4 To generate keypairs for both the system-root-key and the system-enroll-key, enter the following operational mode commands:

```
RP/0/RP0/CPU0:xr9kv-001#crypto key generate rsa system-root-key
Tue Apr 21 22:45:55.400 UTC
The name for the keys will be: system-root-key
Choose the size of the key modulus in the range of 512 to 4096 for your General Purpose Keypair.
Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [2048]:
Generating RSA keys ...
Done w/ crypto generate keypair
[OK]

RP/0/RP0/CPU0:xr9kv-001#crypto key generate rsa system-enroll-key
Tue Apr 21 22:46:24.943 UTC
The name for the keys will be: system-enroll-key
Choose the size of the key modulus in the range of 512 to 4096 for your General Purpose Keypair.
Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [2048]:
Generating RSA keys ...
Done w/ crypto generate keypair
[OK]
RP/0/RP0/CPU0:xr9kv-001#
```

The keys generated are stored securely within the Cisco IOS XR operating system and are not displayed in the configuration.

Step 5 To generate and enroll the certificate required to add the router to Crosswork Cloud Trust Insights, add the following configuration:

```
crypto ca trustpoint system-trustpoint
 keypair rsa system-enroll-key
 ca-keypair rsa system-root-key
 ip-address 1.1.1.1
 subject-name CN=cisco.com
 lifetime certificate 720
 enrollment url self
 message-digest sha256
 lifetime ca-certificate 720
!
```

Note The CA certificate lifetime is set to 2 years (720 days), and the enrollment certificate lifetime is also set to 2 years in the above example.

Step 6 To authenticate and enroll the certificate required for signing operations and enrollment into Crosswork Cloud Trust Insights, enter the following commands:

```
RP/0/RP0/CPU0:xr9kv-001#crypto ca authenticate system-trustpoint
Tue Apr 21 22:47:46.935 UTC
% The subject name in the certificate will include: xr9kv-001.test.cisco.com
  Serial Number  : 25:34
  Subject:
 serialNumber=144c478a,unstructuredName=xr9kv-001.test.cisco.com
Issued By      :
 serialNumber=144c478a,unstructuredName=xr9kv-001.test.cisco.com
  Validity Start : 22:47:47 UTC Tue Apr 21 2020
  Validity End   : 22:47:47 UTC Wed Apr 21 2021
  SHA1 Fingerprint:
  6C20DBEC569808F21A06E779A219C39B1F20E182
RP/0/RP0/CPU0:xr9kv-001#


RP/0/RP0/CPU0:xr9kv-001#crypto ca enroll system-trustpoint
Tue Apr 21 22:48:31.141 UTC

% The subject name in the certificate will include: CN=test.cisco.com
% The subject name in the certificate will include: xr9kv-001.test.cisco.com
% Include the router serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: 144c478a
% The IP address in the certificate is 192.168.23.211
  Serial Number  : 25:35
  Subject:

serialNumber=144c478a,unstructuredAddress=192.168.1.123,unstructuredName=xr9kv-001.test.cisco.com,CN=test.cisco.com

  Issued By      :
 serialNumber=144c478a,unstructuredName=xr9kv-001.test.cisco.com
  Validity Start : 22:48:31 UTC Tue Apr 21 2020
  Validity End   : 22:48:31 UTC Sat Nov 07 2020
  SHA1 Fingerprint:
  8F44F8EE427F9D48B6E47CDF60B90537EF9F65B4
RP/0/RP0/CPU0:xr9kv-001#
```

Step 7 Verify that the signing operations are successfully using the enrollment certificates and keys using the CLI signing utility command as shown in the following example:

Note If the “signature” field is populated, the enrollment certificate is ready for Crosswork Cloud Trust Insights.

```
RP/0/RP0/CPU0:xr9kv-001#show version | utility sign include-certificate
Tue Apr 21 22:49:24.632 UTC
```

```
{
"cli-output": "Cisco IOS XR Software, Version 7.0.2\nCopyright (c) 2013-2020 by Cisco Systems,
Inc.\n\nBuild Information:\n Built By : ahoang\n Built On : Fri Mar 13 22:27:54 PDT 2020\n
Built Host : iox-ucs-029\n Workspace : /auto/srcarchive15/prod/7.0.2/xrv9k/ws\n Version : 7.0.2\n
Location : /opt/cisco/XR/packages/\n Label : 7.0.2\n\ncisco IOS-XRv 9000 () processor\n
System uptime is 8 hours 58 minutes\n\n",
"signature-envelop": {
"signature-version": "01",
"digest-algorithm": "RSA-SHA256",
"pub-key-id": "2508",
"signature":
"F910CRigUmsBBQmnRUoiBYmg+TAWseO1Ey5eRBDwCkT+jHAiQdBhKXGl2MVza5JplrLayDdNbU+L4IvNAlFGegXR1G9IVcd/
RHbsIhhD8GvUTLOrYoIXyWw9b3L0PAbOjRTcbSe5Yr+4qf9XJJ1m88xjtJUgEE08jGz5lYgaBGGHMgS8KwAOmyBiwTaZcKaqYUIiLGqWfJ/
PtxsGv0fhJ+8/9FxjdJcWPLIwXAhQe2QkT15afAjV6LmShQu4TM+Dylad4n4A6YlWFz4sAfEWobl0dVGXPKzDI9UUJDYbdOU8j/
y6Bv9Eko8xYZJaDlUyNCjBWmLi28us9car/wbkfw==",
"signing-certificate": [
"MIIDNDCCAhygAwIBAwICCcswDQYJKoZIhvcNAQELBQAwOzEmMCQGCSqGSIb3DQEJAhYXeHJ2OWtfZXN4MThfNy5
jaXNjby5jb20xETAPBgNVBAUTCGVlZmY1MzRiMB4XDTIxMDIyMDA1NTYzNVoXDTIyMDIyMDA1NTYzNVowOzEmMCQGCSqGSIb3DQEJAhYXeHJ2OWtfZ
XN4MThfNy5jaXNjby5jb20xETAPBgNVBAUTCGVlZmY1MzRiMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0n
LmZqLe9bJNdvpvOFmr8vQzDwZ9pcjtuRx7SOfafs+RasNTnaOot3IL76hayCCfvkCOK/Re/8tUpjDpLS/rtOx9J/adRIK
GjlpYoxK1PK4XxMubg5cOZFzVprQmwur8Rvhx6c2xB79KANqKYSEF4cgoLHMQ0YHkfcBAs9abnStYecUWOGHwnC3OalM1
x3pRe
4ZCY30mS5ZJa/C+21EL+MDCKPj+aUkOCw8ADJUX3qT+TWMf7aLrZj/hfmzDEgrahbv2A1F9QG+ooP53pjRXmN2k6Va67J
tGsZ7spYF8F5KcUF7AhZWvKxGOegS7sUMBu4EhF0eHLoB7Mz3sVGNHNQIDAQABo0IwQDAPBgNVHRMBAf8EBTADAQH/MA4
GA1UdDwEB/wQEAwIBxjAdBgNVHQ4EFgQUFWl+ShMwn/DK+ExWKWVm9JzwJNgwDQYJKoZIhvcNAQELBQADggEBAJvxdPpw
qF0+WHFxvfTzgr09ql7roJ92vao8M47v9xX2pMQFMQceU9tL3O/XZ6sDAg+FF7jyTAOVHgzbfG2OlVoAuDeElgsK5xrYE
RhWBk86IiWTasbrUSeHPNsXJgHK/RuudpB+w8pdOEYORKsVLfFH/u1Sfet33grRkiEvFxU8zj515mnjhVE/4GgeH9hF6T
pR3/1Xv6Afka74wJbikppNo/d2TH4KX6AJ6hKnkd1PGaTyZ
GF1UFOvtFXV5cAwaL0wfUft7qF2YNFr9i4lUuR4oi///c72eLLuL+c00c6hADUH3lJVRTcuaLbsrviz7yEGOD/7/MfYRf
oZ2wNIP2U=", "MIIDhjCCAm6gAwIBAwICCcwwDQYJKoZIhvcNAQELBQAwOzEmMCQGCSqGSIb3DQEJAhYXeHJ2OWtfZXN
4MThfNy5jaXNjby5jb20xETAPBgNVBAUTCGVlZmY1MzRiMB4XDTIxMDIyMDA1NTYzNloXDTIxMDkwODA1NTYzNlowazET
MBEGA1UEAwwKY2lzY28uY29tIDEmMCQGCSqGSIb3DQEJAhYXeHJ2OWtfZXN4MThfNy5jaXNjby5jb20xGTAXBgkqhkiG9
w0BCQgTCjEuNzQuMzIuMzcxETAPBgNVBAUTCGVlZmY1MzRiMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtc
WkoBPwa5yPerZcRtbbUFVDtg7430PjvLzjHjWzmtY/CPea1
bZ3NPWTAUmS0Q+0D5VwqL+5SVkE9ZVwFoRoyMm2+wwbfBAxt0G2MYTdOttLulEP/H7ApVA/Y+pUGXYGsekRxu8Ipyi
Vesi57DQxgHlo2lk4EBsZsDv7oW9Osrtx7rib/kCyA5hTsEpw3oZ20Qp+91QY+vY7NUIQKx78RYkPiQNeOjQqibR0M1Rj
Glgo4ZTDI4IxsdgXm/xxiX3scTqu1q/XVY3v5uEjT2zao0nZAU6z3PQKDSyHDXg3yIDskFMj74HI6hUJsA1U+Qj+mw9DcK
aypjQ8y7zchLeeQQIDAQABo2QwYjAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwID+DAgBgNVHSUBAf8EFjAUBgg
rBgEFBQcDAQYIKwYBBQUHAwIwHQYDVR0OBBYEFHJJ3dCXoGGWD2yZ8JQ3f/A/8XqxMA0GCSqGSIb3DQEBCwUAA4IBAQBm
z5YfGTbNAXPHJCxA9w8HUHyr1MlKB6wMKT0AUoWBJ6HvXJXoA
H5cs7uF3Zw4QjY28HaaxkMPr6338VbGi3DnyIOf1Hc6/XRfNBi3eMYcSNyRRgtvQSmTzM7A3CrSOiFlMmdPCdYIeoFiMd
M3uIZzfMe1EnONetev1bs+Te29utYXzb6QWjW0oJZ6/6g4cauo6jkhC/SNsRh3b/+8YMzxAHgzRFg+rm/O6cYa3jNCopjR
JqeFfmNuISgU9LIszmkt3/4n4uiAj4aAqwAc7YG0dzwWdwiXUwj3Q7TrMS8R8AaLUN47nYzm0QfUwNbUDkST2XjIGV90J
vH3E2CnAX+j" ]
}
}
```


This verifies your router is configured correctly in order to have trust information retrieved.

Step 8 If you encounter problems with the signing operation, use the following commands to clear the existing certificates and keys:

```
# crypto key zeroize rsa <name of key>
# clear crypto ca certificates system-trustpoint
# crypto ca cancel-enroll system-trustpoint
```

Step 9 To renew a certificate before it expires, use the following commands:

```
# clear crypto ca certificate system-trustpoint
# crypto key zeroize rsa system-enroll-key
# crypto key generate rsa system-enroll-key
# crypto ca authenticate system-trustpoint
# crypto ca enroll system-trustpoint
```

Note Regenerate the enrollment key prior to renewing the certificate. The lifetime for the signing CA certificate and the enrollment certificate is set using the **crypto ca trustpoint** configuration.

Configure Limited Privilege User for Crosswork Trust Insights

To prevent unauthorized operational or configuration changes to your Cisco IOS XR routers, the credentials used to access the devices should have limited privileges. Ensure your devices have the following configuration, which includes the recommended taskgroup and user configuration, to allow the minimal authorization required to execute the trust dossier and signing commands.

The following commands are supported in release Cisco IOS XR Release 7.3.1 and later:

```
!
taskgroup alltasks-dossier
task read sysmgr
task read system
task read dossier
task read pkg-mgmt
task read basic-services
task read config-services
task execute dossier
task execute basic-services
!
```

The following commands are supported in releases prior to Cisco IOS XR Release 7.3.1:

```
!
taskgroup alltasks-dossier
 task read sysmgr
 task read system
 task read pkg-mgmt
 task read basic-services
 task read config-services
 task execute crypto
 task execute dossier
 task execute basic-services
!
usergroup dossier-group
 taskgroup alltasks-dossier
!
username dossier
 group dossier-group
 secret 10 <not shown here>
!
```

This configuration creates:

- The **alltasks-dossier** task group, which defines all required tasks to enable dossier collection and signing operations. You can rename the task group if needed.
- The **dossier-group** user group, which is where the task permissions are assigned. You can rename the user group name if needed.
- The **dossier** user with the appropriate taskgroup permissions. You can rename the user if needed. Make sure you specify the appropriate credentials (secret).

After applying this configuration, you can create a new credential group in Crosswork Cloud Trust Insights with this information. See Create Credentials for more information.

Add Devices

Complete the following steps to add your devices.

Before you begin

- There must be at least one active data gateway in Crosswork Cloud.
- When using a CSV file to import devices:
  - if any optional fields are listed in the CSF file (credentials, device groups, or data gateways), confirm that they are configured prior to adding the devices:
    - Credentials (**Configure** > **Credentials**)
    - Device Groups (**Configure** > **Device Groups**)
    - Data Gateways (**Configure** > **Data Gateways**)
  - up to 1,000 devices can be imported in one operation, and
  - you can download a sample CSV file to edit and use (**Configure** > **Devices** > **CSV Import** tab).

Step 1 In the main window, click **Configure** > **Devices**. You can also add a device and link it to a Crosswork Data Gateway by navigating to **Configure** > **Data Gateways** > ***data_gateway_name***.

Step 2 Click **Add Device**.

Step 3 To import devices using a CSV file, click **CSV Import**.

Step 4 To import a single device, complete the following fields:

Table 25: Add Device Field Descriptions

Field	Description
Device Name	Display name of the device. **Note** For data privacy reasons, this field isn't automatically populated from the device.
Description	(Optional) Add a description of the device.
Hostname	The DNS FQDN or IP address that is used by Crosswork Data Gateway.
SSH Port	(Optional) TCP port for SSH access. The default is TCP/22. SSH access is not required for Crosswork Cloud Traffic Analysis.
Credential: SSH	If you previously created a credential group, you can select it from the **Credential: SSH** drop-down list. To create a new credential group, from the **Credential: SSH** drop-down list, select **Add New Credential**. For more information about credential groups, see Create Credentials, on page 189.

Field	Description
Device Group	For Crosswork Cloud Traffic Analysis only. If you previously created a device group, you can select it from the **Device Group** drop-down list. To create a new device group, from the **Device Group** drop-down list, select **Add new device group**. For more information about device groups, see Configure Device Groups, on page 191.
City	(Optional) City for device geo-location.
Location	(Optional) Logical site identifier.
Country	(Optional) Country for device geo-location.
Device Timezone	(Optional) Timezone local to device.
Tags	(Optional) Specify a tag to help with grouping and identifying devices. For example, you might want to enter text that identifies router types in your system, such as *edge*.

The remaining fields depend on the Crosswork Cloud applications for which you have a valid license. You have the option to link a device to both a Crosswork Data Gateway instance for Crosswork Cloud Trust Insights and a Crosswork Data Gateway instance for Crosswork Cloud Traffic Analysis.

Table 26: Trust Insights Add Device Field Descriptions

Field	Description
Data Gateway: Trust Insights	Toggle the switch to **On** and select a Crosswork Data Gateway instance for the device. To add a Crosswork Data Gateway, see Add Crosswork Data Gateway Information.
Collect Configuration Hash	Enables collection of configuration hash information. This must be set to **Yes** if you want to include the Device Running Configuration alarm which monitors possible unwanted device configuration changes. When enabled, Crosswork Trust Insights checks to see if the stored hash does not match the hash reported by the system.
Configuration Hash Collection Frequency	From the drop-down list, select the interval you want Crosswork Trust Insights to collect the device hash configuration.

Table 27: Traffic Analysis Add Device Field Descriptions

Field	Description
Data Gateway: Traffic Analysis	Toggle the switch to **On** and select a NetFlow Data Gateway instance for the device.
NetFlow Source Address	Enter the NetFlow source address.
ASN	Enter the ASN. The value must be in the private ASN range (64512 - 65535).
SNMP Address	If you do not enter an SNMP address, the NetFlow address is used.

Field	Description
Credential: SNMP	If you previously created a credential group, you can select it from the **Credential: SNMP** drop-down list. To create a new credential group for the device you're adding, from the **Credential: SNMP** drop-down list, select **Add New Credential**. For more information about credential groups, see Create Credentials, on page 189.
BGP Router ID IP Address	—
Credential: BGP	If you previously created a credential group, you can select it from the **Credential: BGP** drop-down list. To create a new credential group for the device you're adding, from the **Credential: BGP** drop-down list, select **Add New Credential**. For more information about credential groups, see Create Credentials, on page 189.

Note All BGP prefixes must be shared with Cisco Crosswork Data Gateway.

Step 5 Click **Save**.

After the save operation completes, the device appears when you click **Monitor** > **Devices** or **Configure** > **Devices** in the main window.

Trust Dossier Information for Trust Insights

After you add a device to Crosswork Cloud Trust Insights, a dossier containing trust information is retrieved from the routers via Crosswork Data Gateway. The trust dossier (.json format) is collected via SSH and is signed with a Crosswork Cloud Trust Insights enrollment key. The trust dossier that Crosswork Data Gateway forwards to Crosswork Cloud Trust Insights contains the following information:

- Cisco IOS version and platform output
- Anti-replay nonce
- System hardware inventory
- File system inventory

Note The File system inventory is supported in Cisco IOS XR Release 7.9.1 and later releases.

- Secure unique device identifier (SUCI) certificate for hardware identify
- Software package inventory
- Reboot history
- Rollback history

Collect Data for Trust Insights Device Dossier

The following procedure describes how to initiate an ad hoc dossier collection to get the latest device information. By default, device dossier collection occurs every 12 hours. To change the dossier collection frequency or disable collection for one or more devices, see Change Device Dossier Collection Frequency, on page 167.

Step 1 In the main window, click **Trust Insights** > **Configure** > **Devices**.

Step 2 Click on the name of the device for which you want to force a dossier collection.

Step 3 Click the **Trust Insights** tab.

Step 4 Click **Collect Dossier**.

An informational message appears indicating it may take a few minutes to complete the dossier collection, and text appears under the **Collect Dossier** button about the request.

After the dossier collection is complete, the device data on the UI is updated.

Change Device Dossier Collection Frequency

You can change the dossier collection frequency for one or more devices.

Note This procedure applies to Crosswork Cloud Trust Insights devices only.

Step 1 In the main window, click **Trust Insights** > **Configure** > **Devices**.

Step 2 Check the checkbox next to one or more devices for which you want to change the frequency of the dossier collection.

Step 3 Click **Collection**.

Note Crosswork Cloud displays Trust Insights devices only. If you select a device that doesn't belong to Trust Insights, it will not be displayed.

Step 4 Confirm that the **Disabled/Enabled** toggle switch is set to **Enabled**. Selecting **Disabled** stops any future dossier collections.

Step 5 From the **Frequency** drop-down list, select the frequency in which you want the collection performed. Notice that the device **New Frequency** and **New Status** columns are updated appropriately.

Step 6 Click **Save**.

Troubleshoot Crosswork Data Gateway and Device Connectivity for Trust Insights

The following steps explain how to troubleshoot connectivity between Crosswork Data Gateway and your Crosswork Cloud Trust Insights devices.

Step 1 In the main window, click **Devices** and then click the device for which you want to view connectivity to Crosswork Data Gateway.

Step 2 Click the **Status** tab.

Step 3 If the connection between the Crosswork Data Gateway and the device are red, indicating there is an error, ensure that if you have a firewall, it is configured to allow cdg.crosswork.cisco.com and crosswork.cisco.com.

Test and correct the connectivity between Crosswork Data Gateway and the device.

Step 4 Ensure the **SSH** arrow between the Crosswork Data Gateway and the device is green, indicating that the connection is working.

If the **SSH** arrow is red, Crosswork Data Gateway is not able to connect to the device. Correct the following errors:

- Ensure the SSH configuration on the router is correct. See Verify Router Configuration for Crosswork Trust Insights, on page 159 for more information.
- Ensure that the credentials you entered in Crosswork Cloud Trust Insights match the credentials configured on the router. Hover your cursor over the **SSH** link and click the blue hyperlink to go to the credentials for that device.

Step 5 Ensure the **Trust Data** arrow between the Crosswork Data Gateway and the device is green, indicating that the connection is working.

Disable Devices

When you disable a device, the collection of information temporarily stops. The previously collected device data is retained.

Alternatively, you can *remove* a device to remove it and its data completely. You cannot recover any of its data after removing a device. See Delete Devices, on page 168.

Step 1 In the main window, click **Monitor** > **Devices** or **Configure** > **Devices**.

Step 2 Select the check box next to one or more devices you want to deactivate, then click **Disable**.

A message appears to indicate that the device is deactivated.

You can reactivate a device that you previously deactivated. After reactivating a device, it can take up to 30 mins for the statistics to appears on the device details page.

Step 3 To restart data collection for the device, select the device, then click **Enable**.

A message appears to indicate that the device is activated, and data collection for the device resumes.

Delete Devices

When you delete a device, the system deletes all previously collected device data. You have up to seven days to recover device data.

Alternatively, you can Disable Devices a device to temporarily stop the data collection and retain previously collected device data.

Step 1 In the main window, click **Monitor > Devices** or **Configure > Devices**.

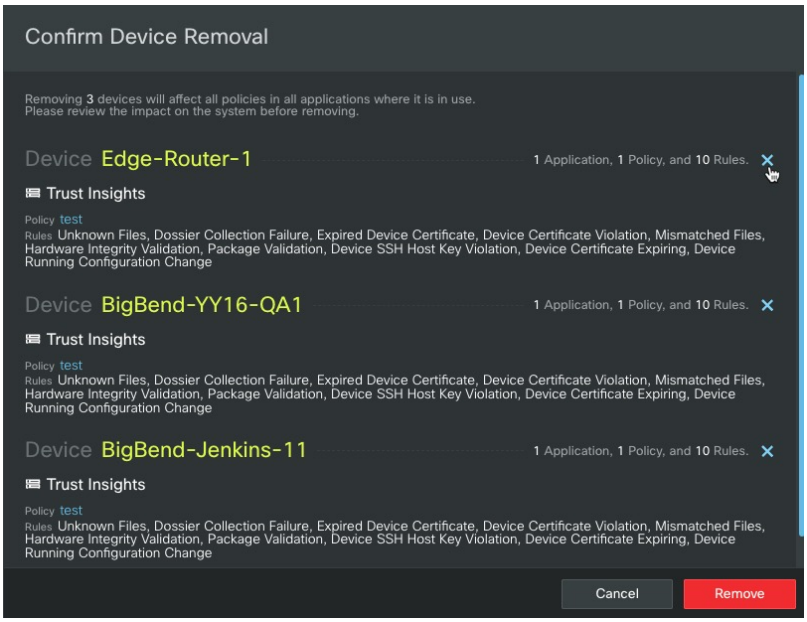
Step 2 Click the checkbox next to the name of one or more devices you want to delete.

Step 3 Click **Remove**. A confirmation window appears listing all applications, policies, and rules that will be impacted.

Step 4 If you selected more than one device and decide to exclude any devices from removal, click the **x** next to the device entry.

Example:

Figure 5: Delete Device Confirmation



Step 5 To confirm device deletion, click **Remove**.

The device, and its previously collected data, is deleted.

Step 6 To restore a recently removed device, see Restore Removed Devices, on page 169.

Restore Removed Devices

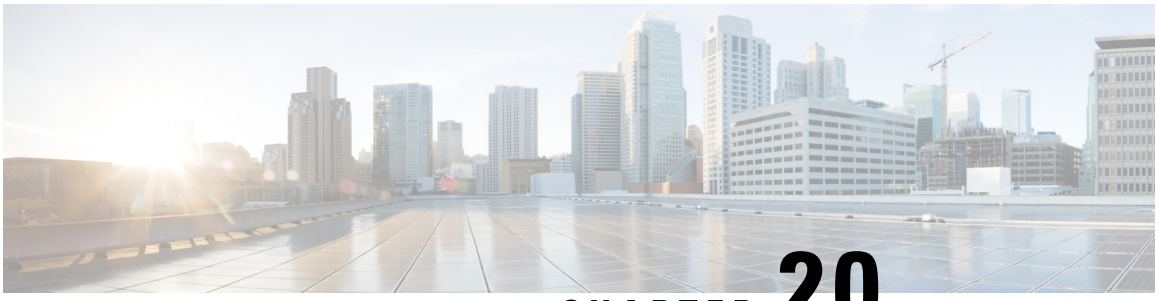
You can restore a previously removed device. When you remove a device, Crosswork Cloud remembers the device for approximately 7 days to allow you to readd it quickly if needed.

Step 1 In the main window, click **Configure > Removed Devices**.

If it has been longer than 7 days since you removed the device, it might not appear on the list of Removed Devices. You will have to re-add the device as described in Add Devices, on page 164.

Step 2 Click **Restore** next to the device you want to re-add.

The device is restored.



CHAPTER 20

Configure Crosswork Data Gateways

Manage Crosswork Data Gateways

Cisco Crosswork Data Gateway(s) collect information from managed devices and send it to Crosswork Cloud. You must first install Crosswork Data Gateway (Data Gateway) before you can use Trust Insights or Traffic Analysis. A Data Gateway is initially deployed as a VM called Base VM that contains only enough software to enroll itself with Crosswork Cloud. Once the Data Gateway is registered with Crosswork Cloud, Crosswork Cloud pushes the collection job configuration down to the Data Gateway, enabling it to gather the data it needs from the network devices.

To view, edit, or add a Data Gateway, go to  or  > **Configure** > **Data Gateways**.

This page lists the current status and details of all Data Gateways registered in Crosswork Cloud.

Table 28: Manage Data Gateways

Task	Notes
To add a new Data Gateway, click **Add Data Gateway**.	Add Crosswork Data Gateway Information, on page 17 For a high-level summary of steps on how to register Crosswork Data Gateway to Traffic Analysis or Trust Insights, see one of the following topics: • Workflow: Add a Crosswork Data Gateway to Crosswork Cloud Traffic Analysis , on page 173 • Workflow: Add a Crosswork Data Gateway to Crosswork Cloud Trust Insights , on page 175
To delete a Data Gateway, check the check box next to the Data Gateway you want to delete, then click **Remove**.	This task removes the Data Gateway completely. Data Gateway information is not retained.
To disable a Data Gateway from sending network data to Crosswork Cloud, click on the Data Gateway name, then click **Disable**.	When a Data Gateway is disabled, the Data Gateway information is retained.
To modify a Data Gateway, click on the Data Gateway name, then click **Edit**.	You can update the name, description, ASN, or register the Data Gateway to another application (Trust Insights or Traffic Analysis). **Note** Prior to registering the Data Gateway to another application, you must unlink all devices from the currently registered application.
To check the status of collection and the next upcoming collection interval, click on the Data Gateway name, then click the **Overview** tab.	—
To add, link, or unlink devices from the Data Gateway, click on the Data Gateway name, then click the **Linked Trust / Traffic Devices** tab.	• Add Devices, on page 164 • Link Devices to Crosswork Data Gateway, on page 183
To view pending Data Gateway tokens, click the **Pending Enrollment** tab.	After a Data Gateway is created with a valid enrollment token, it will appear here in pending state. To continue, click **Allow** under the Action column for the Data Gateway you wish to add. **Note** This step is also part of registering a Data Gateway to Crosswork Cloud. For more information, see Add Crosswork Data Gateway Information, on page 17.

Task	Notes
To manage Data Gateway tokens, click the **Manage Tokens** tab.	This page displays enrollment token details. From this page you can create a new enrollment token or select an existing token to view the enrollment token passcode, or revoke the token. **Note** This step is also part of registering a Data Gateway to Crosswork Cloud. For more information, see Add Crosswork Data Gateway Information, on page 17.

Workflow: Add a Crosswork Data Gateway to Crosswork Cloud Traffic Analysis

The following is a high-level summary of steps that must be performed when adding Crosswork Data Gateway to Crosswork Cloud Traffic Analysis.

Note To help confirm your environment is set up, you can also use the Crosswork Cloud Traffic Analysis Setup Checklist (> **Setup Checklist**)

Table 29: Add Crosswork Data Gateway to Crosswork Cloud Traffic Analysis Workflow

Step	Action	Crosswork Cloud Navigation and Notes
1	Confirm Crosswork Data Gateway requirements.	Installation Requirements
2	Gather information needed during Crosswork Data Gateway installation. Make sure you have the following: • A network where Crosswork Data Gateway can connect to Crosswork Cloud (Management Interface) • A network where Crosswork Data Gateway can connect to the devices (optional Southbound Interface) • IP address information for each interface • A proxy, if it is required to connect to the internet	Deployment Parameters and Scenarios

Step	Action	Crosswork Cloud Navigation and Notes
3	• For Crosswork Data Gateway 6.0.1 or later: Create and copy an enrollment token (.json registration file) to use during Crosswork Data Gateway installation. The .json registration file contains unique digital certificates that are used to enroll Crosswork Data Gateway into Crosswork Cloud. • For Crosswork Data Gateway versions earlier than 6.0.1, follow the steps described in Manually Add Crosswork Data Gateway Information, then go to Step 6.	Add Crosswork Data Gateway Information For Crosswork Data Gateway 6.0.1 or later: 1. > **Data Gateways** > **Use Enrollment Token** 2. Create or select an enrollment token. 3. Copy the enrollment token somewhere so that it is readily available when you install Crosswork Data Gateway. **Note** After you copy the enrollment token, you will need to install Crosswork Data Gateway before you can continue in Crosswork Cloud Traffic Analysis.
4	Install Crosswork Data Gateway. During Crosswork Data Gateway installation, you will need to paste the enrollment token in the following platforms: • VMware • vCenter vSphere Client—Paste the token text into the **Auto Enrollment Package Transfer** > **Enrollment Token UI** field • OVF Tool—Locate the script and under the `## Enrollment Token for Crosswork Cloud` section, paste the token text after `CloudEnrollmentToken=` • OpenStack—Locate the config.txt file and under the `## Enrollment Token for Crosswork Cloud` section, paste the token text after `CloudEnrollmentToken=` • Amazon EC2—Paste the token in the CloudFormation template or as part of the user data after `CloudEnrollmentToken=`	Install Crosswork Data Gateway

Step	Action	Crosswork Cloud Navigation and Notes
5	Authorize Crosswork Data Gateway access to Crosswork Cloud Traffic Analysis. **Note** Each Crosswork Data Gateway can be applied to one Crosswork Cloud Traffic Analysis application only. This means that you cannot use *this instance* of Crosswork Data Gateway for Crosswork Cloud Trust Insights.	1. > **Data Gateways** > **Use Enrollment Token** 2. Click **Next**. The newly installed Crosswork Data Gateway should appear with then Enrollment State as **Pending**. 3. Click **Allow** to authorize the Crosswork Data Gateway access.
6	Configure BGP, SNMP, and network flow monitoring protocols on devices for Crosswork Cloud Traffic Analysis.	Prerequisites for Adding Devices for Traffic Analysis
7	Add device credentials for BGP, SSH (optional), and SNMP to be used when adding devices.	Create Credentials > **Configure** > **Credentials** > **Add Credential**
8	Add devices. **Note** If devices have already been added in Crosswork Cloud, you can simply link them to Crosswork Cloud Traffic Analysis. > **Data Gateways** > ***data-gateway-name*** > **Linked Traffic Devices** tab	• Add Devices > **Configure** > **Devices** > **Add Device** • Confirm all connections are up. > **Configure** > **Devices** > ***device_name*** > **Status** tab
9	Designate an external interface. Crosswork Cloud Traffic Analysis cannot display traffic data until you designate an external interface to connect to the internet.	Designate an External Interface > **Configure** > **Devices** > ***device_name*** > **Traffic Analysis** tab > **Interfaces**

Workflow: Add a Crosswork Data Gateway to Crosswork Cloud Trust Insights

The following is a high-level summary of steps that must be performed when adding Crosswork Data Gateway to Crosswork Cloud Trust Insights.

Table 30: Add a Crosswork Data Gateway to Crosswork Cloud Trust Insights Workflow

Step	Action	Crosswork Cloud Navigation and Notes
1	Confirm Crosswork Data Gateway requirements.	Installation Requirements
2	Gather information needed during Crosswork Data Gateway installation. Make sure you have the following: • A network where Crosswork Data Gateway can connect to Crosswork Cloud (Management Interface) • A network where Crosswork Data Gateway can connect to the devices (optional Southbound Interface) • IP address information for each interface • A proxy, if it is required to connect to the internet	Deployment Parameters and Scenarios
3	• For Crosswork Data Gateway 6.0.1 or later: Create and copy an enrollment token (.json registration file) to use during Crosswork Data Gateway installation. The .json registration file contains unique digital certificates that are used to enroll Crosswork Data Gateway into Crosswork Cloud. • For Crosswork Data Gateway versions earlier than 6.0.1, follow the steps described in Manually Add Crosswork Data Gateway Information, on page 180, then go to Step 6.	Add Crosswork Data Gateway Information, on page 17 For Crosswork Data Gateway 6.0.1 or later: 1.  **> Data Gateways > Use Enrollment Token** 2. Create or select an enrollment token. 3. Copy the enrollment token somewhere so that it is readily available when you install Crosswork Data Gateway. **Note** After you copy the enrollment token, you will need to install Crosswork Data Gateway before you can continue in Crosswork Cloud Trust Insights.

Step	Action	Crosswork Cloud Navigation and Notes
4	Install Crosswork Data Gateway. During Crosswork Data Gateway installation, you will need to paste the enrollment token in the following platforms: • VMware • vCenter vSphere Client—Paste the token text into the **Auto Enrollment Package Transfer > Enrollment Token UI** field • OVF Tool—Locate the script and under the `## Enrollment Token for Crosswork Cloud` section, paste the token text after `CloudEnrollmentToken=` • OpenStack—Locate the config.txt file and under the `## Enrollment Token for Crosswork Cloud` section, paste the token text after `CloudEnrollmentToken=` • Amazon EC2—Paste the token in the CloudFormation template or as part of the user data after `CloudEnrollmentToken=`	Install Crosswork Data Gateway
5	Authorize Crosswork Data Gateway access to Crosswork Cloud Trust Insights. **Note** Each Crosswork Data Gateway can be applied to one Crosswork Cloud application only. This means that you cannot use *this instance* of Crosswork Data Gateway for Crosswork Cloud Traffic Analysis.	1. > **Data Gateways > Use Enrollment Token**. 2. Click **Next**. The newly installed Crosswork Data Gateway should appear with then Enrollment State as **Pending**. 3. Click **Allow** to authorize the Crosswork Data Gateway access.
6	Confirm you have all the Cisco IOS XR supported images, enrollment keys, certificates, and requirements needed for Crosswork Cloud Trust Insights.	• Cisco IOS XR Supported Images • Verify Router Configuration
7	Configure a user with limited access to devices for Crosswork Trust Insights to prevent unauthorized operational or configuration changes to your Cisco IOS XR routers.	Configure Limited Privilege User
8	Add device credential profiles to be used when adding devices.	Create Credentials > **Configure > Credentials > Add Credential**

Step	Action	Crosswork Cloud Navigation and Notes
9	Add devices. **Note** If devices have already been added in Crosswork Cloud, you can simply link them to Crosswork Cloud Trust Insights (> **Data Gateways** > ***data-gateway-name*** > **Linked Trust Devices** tab).	• Add Devices **Devices** > **Add Device** • Confirm all connections are up. **Devices** > ***device_name*** > **Status** tab **Note** You must have the following information populated: • Name • Hostname • Device timezone • Data Gateway • Credential group (defined in previous step)
10	Give it some time to collect data, then verify that the device data collection was successful.	> **Monitor** > **Devices** > ***device-name*** **Trust Insights** tab
11	(Optional) Initiate a dossier collection to get the latest device information	Collect Data for Trust Insights Device Dossier > **Configure** > **Devices** > ***device-name*** > **Trust Insights** > **Collect Dossier**

Add Crosswork Data Gateway Information

As part of the Data Gateway deployment process, an enrollment token (a unique registration file) must be created to enroll the Crosswork Data Gateway into Crosswork Cloud.

Starting with Crosswork Data Gateway 6.0.1, an enrollment token can be created in the Crosswork Cloud UI and then embedded during VM installation. The .json registration file contains unique digital certificates that are used to enroll the Crosswork Data Gateway into Crosswork Cloud. This method automatically enrolls a Crosswork Data Gateway in Crosswork Cloud and is less prone to potential problems than the older method.

For Crosswork Data Gateway versions earlier that 6.0.1, you must first Install Crosswork Data Gateway, generate an enrollment token from the Crosswork Data Gateway interactive console, and then manually enter Crosswork Data Gateway information in Crosswork Cloud.

Note

- While the procedure documented here describes the steps to use the newer method (if you are using Crosswork Data Gateway 6.0.1 or later), you have the option to use the older method (see Manually Add Crosswork Data Gateway Information, on page 180).
- If you use a firewall on your Data Gateway egress traffic, ensure that your firewall configuration allows cdg.crosswork.cisco.com and crosswork.cisco.com.

Step 1 From the main window, navigate to or > **Configure** > **Data Gateways** and then click **Add Data Gateway**.

Step 2 Choose to do one of the following:

- For Crosswork Data Gateway 6.0.1 and later, continue to Step 3.
- For earlier Crosswork Data Gateway versions, click **Registration File** and go to Manually Add Crosswork Data Gateway Information, on page 180.
- If you need to download the latest supported Crosswork Data Gateway version, click **Download CDG Image**.

Step 3 Click **Use Enrollment Token**.

Step 4 You can create a new token or use an existing one. Do one of the following:

- **Create a new token**
  - **a.** Click **Create Enrollment Token**.
  - **b.** Enter the following:
    - **Token Name**: Specify a unique name to the token that you are creating.
    - **Description**: Enter a detailed description of the token.
    - **Number of Uses**: Specify the permissible number of token uses. The maximum token usage limit is 50.
    - **Valid Until**: Specify the validity period for the token. The maximum duration is 366.
  - **c.** Click **Create**.
- **Use an existing token**
  - **a.** Select the row corresponding to the token that you intend to use.

    When selecting an existing token, consider its expiration date. If the Data Gateway will not be installed and registered prior to the expiration date, Cisco recommends you avoid using that token.

    You can review the **Valid Until** column on the **Add Crosswork Data Gateway** page to determine the expiration information.
  - **b.** Click **View Enrollment Token**.
    - **Token Name**: Specify a unique name to the token that you are creating.
    - **Description**: Enter a detailed description of the token.
    - **Number of Uses**: Specify the permissible number of token uses. The maximum token usage limit is 50.

- **Valid Until**: Specify the validity period for the token. The maximum duration is 366.

c. Click **Create**.

Step 5 Click **Copy** to copy the token. Paste the content in a local file. During Crosswork Data Gateway installation, you will need to paste the enrollment token in the following platforms:

- VMware
  - vCenter vSphere Client—Paste the token text into the **Auto Enrollment Package Transfer > Enrollment Token UI** field
  - OVF Tool—Locate the script and under the `## Enrollment Token for Crosswork Cloud` section, paste the token text after `CloudEnrollmentToken=`
- OpenStack—Locate the config.txt file and under the `## Enrollment Token for Crosswork Cloud` section, paste the token text after `CloudEnrollmentToken=`
- Amazon EC2—Paste the token in the CloudFormation template or as part of the user data after `CloudEnrollmentToken=`

Step 6 Install Crosswork Data Gateway.

Step 7 After Crosswork Data Gateway is installed, navigate back to > **Data Gateways > Use Enrollment Token**.

Step 8 Click **Next**. The newly installed Crosswork Data Gateway should appear with the Enrollment State as **Pending**.

Step 9 Click **Allow** to authorize the Crosswork Data Gateway access.

Step 10 Click **Next** after reviewing the Device information.

Step 11 Click **Accept** after reviewing the Network information.

Step 12 After a few minutes, verify that your Crosswork Data Gateway is successfully connected. Click **Data Gateways**, click on the name of the Crosswork Data Gateway, and verify the following values for the Crosswork Data Gateway you added:

- **Connectivity**: Session Up
- **Admin State**: Enabled
- **Container Image**: Matched

You may need to refresh the page to see the changes.

Manually Add Crosswork Data Gateway Information

Note If you use a firewall on your Crosswork Data Gateway egress traffic, ensure that your firewall configuration allows cdg.crosswork.cisco.com and crosswork.cisco.com.

Before you begin

For Crosswork Data Gateway versions earlier that 6.0.1, you must first install Crosswork Data Gateway, generate an enrollment token from the Crosswork Data Gateway interactive console, and then manually enter Crosswork Data Gateway information in Crosswork Cloud. For more information, see the following:

1. Install Crosswork Data Gateway
2. Obtain and Export Enrollment Package

Step 1 From the main window, do one of the following:

- For Crosswork Cloud Traffic Analysis, navigate to > **Configure > Data Gateways** and then click **Add Data Gateway**.
- For Crosswork Cloud Trust Insights, navigate to > **Configure > Data Gateways** and then click **Add Data Gateway**.

Step 2 Click **Registration File** to upload the enrollment data file you downloaded from Crosswork Data Gateway, navigate to the location of the .json file, then click **Next**.

Step 3 Enter a name for the Crosswork Data Gateway.

Step 4 In the Application field, confirm that the applicable Crosswork Cloud application for which you're using this Crosswork Data Gateway instance is the correct one. Each Crosswork Data Gateway can be applied to one Crosswork Cloud application only.

Step 5 Complete the rest of the required fields, then click **Next**.

Step 6 (Optional) Type a tag name and click New Item (or select from existing tag names), which allows you to group Crosswork Data Gateways with the same tag, then click **Next**.

Step 7 If you have more than one NIC and you want a NIC to talk to southbound traffic, you would configure it in this window.

Step 8 Review the Crosswork Data Gateway information that you entered, then click **Next**.

Step 9 Click **Accept** to accept the security certificate.

A message appears to indicate the Crosswork Data Gateway was successfully added.

Step 10 After a few minutes, verify that your Crosswork Data Gateway is successfully connected. Click **Data Gateways**, click on the name of the Crosswork Data Gateway, and verify the following values for the Crosswork Data Gateway you added:

- **Connectivity**: Session Up
- **Admin State**: Enabled
- **Container Image**: Matched

You may need to do a refresh to see the changes.

Install Crosswork Data Gateway

Crosswork Data Gateway is required for Crosswork Cloud Traffic Analysis and Crosswork Cloud Trust Insights only. It is not required for Crosswork Cloud Network Insights.

Prior to Crosswork Data Gateway installation, review the steps outlined in one of the following topics:

- Workflow: Add a Crosswork Data Gateway to Crosswork Cloud Trust Insights , on page 175
- Workflow: Add a Crosswork Data Gateway to Crosswork Cloud Traffic Analysis , on page 173

Note For Crosswork Data Gateway 6.0.1 and later, you have the option to create an enrollment token within Crosswork Cloud and then install a Crosswork Data Gateway. For earlier Crosswork Data Gateway versions, you must install a Crosswork Data Gateway first and manually enter the Data Gateway information in Crosswork Cloud.

Install a Crosswork Data Gateway as explained in the Cisco Crosswork Data Gateway Installation and Configuration Guide for Cloud Applications.

View Data Gateway Health

You can quickly view the health of your Crosswork Data Gateway instances. From the main window under **Configure**, click **Data Gateways**. Click on the Crosswork Data Gateway instance you want to view the health.

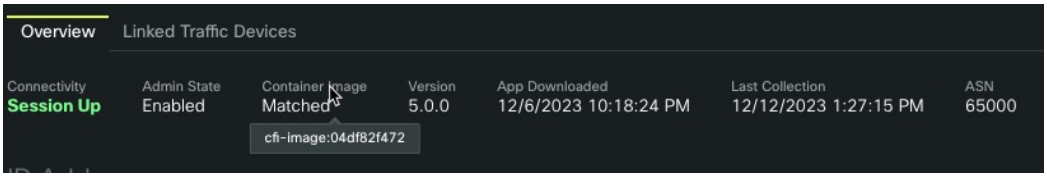
The Crosswork Data Gateway collection and health information are displayed. You can view connectivity status, when the application was downloaded, and when the last data collection occurred.

The **Container Image** field indicates the Docker image status using the following values:

- **Matched**—The Data Gateway is running the latest published Docker image.
- **Mismatched**—The Data Gateway is running an older Docker image.
- **Missing**—A Docker image has not been downloaded.

You can also hover your mouse over the **Container Image** field to view the Docker image tag.

Figure 6: View Data Gateway Health



Link Devices to Crosswork Data Gateway

You can select a Crosswork Data Gateway instance to collect the dossier for each device you added. You must add a Data Gateway before performing this task.

Step 1 From the main window, click **Data Gateways**.

Step 2 Click on the Data Gateway instance you want to link to a device.

Step 3 Click the **Linked Trust / Traffic Devices** tab.

A list of any devices that were previously linked to the Data Gateway is displayed.

Step 4 Select the devices to link to the Data Gateway, then click **Link Traffic Devices**.

After devices are linked to a Data Gateway, they are automatically scheduled for collection. To check the status of collection and the next upcoming collection interval, look at the **Overview** tab on the Data Gateway page.

Note To unlink devices, check the box for one or more devices that you want to unlink, then click **Unlink**. The Data Gateway will no longer collect the dossier for the device you unlinked.

Troubleshoot Crosswork Data Gateway and Device Connectivity for Traffic Analysis

The following steps explain how to troubleshoot connectivity between Crosswork Data Gateway and your Crosswork Cloud Traffic Analysis devices.

Step 1 In the main window, click **Devices** and then click the device for which you want to view connectivity to Crosswork Data Gateway.

Step 2 Click the **Status** tab.

Step 3 If all of the connections between the Crosswork Data Gateway and the device are red, indicating there is an error, ensure that if you have a firewall, it is configured to allow cdg.crosswork.cisco.com and crosswork.cisco.com.

Test and correct the connectivity between Crosswork Data Gateway and the device.

Step 4 Ensure the **SNMP** arrow between the Crosswork Data Gateway and the device is green, indicating that the connection is working.

If the **SNMP** arrow is red, Crosswork Data Gateway is not able to connect to the device. Correct the following errors:

- Ensure the SNMP configuration on the router is correct. See SNMP Configuration Examples, on page 153 for more information.
- Ensure that the credentials you entered in Crosswork Cloud Traffic Analysis match the credentials configured on the router. Hover your cursor over the **SNMP** link and click the blue hyperlink to go to the credentials for that device.
- If you created an SNMP view, ensure you specified the correct SNMP object identifiers (OIDs). See SNMP Object Identifiers Used by Traffic Analysis, on page 157.

- Verify that you entered the correct SNMP IP address. Click **Edit**, then scroll to the Crosswork Cloud Traffic Analysis section and verify the **SNMP Address** field.

Step 5 Ensure the **BGP** arrow between the Crosswork Data Gateway and the device is green, indicating that the connection is working.

If the **BGP** arrow is red, correct the following errors:

- Check that the IP address for the BGP peer is correct. Click **Edit**, then scroll to the Crosswork Cloud Traffic Analysis section and verify the **BGP Router ID IP Address** field.
- If you're using credentials for BGP, make sure the credentials you entered in Crosswork Cloud Traffic Analysis match the credentials configured on the router.
- Ensure that your device configuration includes the IP address of the Crosswork Data Gateway and the ASN of the Crosswork Data Gateway (the default ASN is 65000) and that they are neighbors.
- Ensure that the BGP session between the Crosswork Data Gateway and the device is an external BGP (e-BGP) session.

Note The **SSH** connection between the Crosswork Data Gateway and the device is not required for Crosswork Cloud Traffic Analysis.

Step 6 Ensure the **Traffic Data** arrow between the Crosswork Data Gateway and the device is green, indicating that the connection is working.

If the **Traffic Data** arrow between the Crosswork Data Gateway and the device is red, check the NetFlow configuration on your router, specifically the port number (255) and the IP address from where the NetFlow data is being exported. Ensure the IP address you specified in the **NetFlow Source Address** field matches the IP address from where the NetFlow records are being exported.

Step 7 If all connections are green and you are not seeing traffic data, ensure you have correctly configured internal and external interfaces. See Designate an External Interface for Crosswork Traffic Analysis, on page 158.

Disable Crosswork Data Gateways

You can deactivate a Crosswork Data Gateway, which retains the Crosswork Data Gateway information, but disables the Crosswork Data Gateway from sending network data to Crosswork Cloud.

To delete a Crosswork Data Gateway and remove it and its data completely, see Delete Crosswork Data Gateways, on page 185.

Step 1 From the main window, click **Data Gateways**.

Step 2 Click on the Crosswork Data Gateway instance you want to deactivate, then click **Disable**.

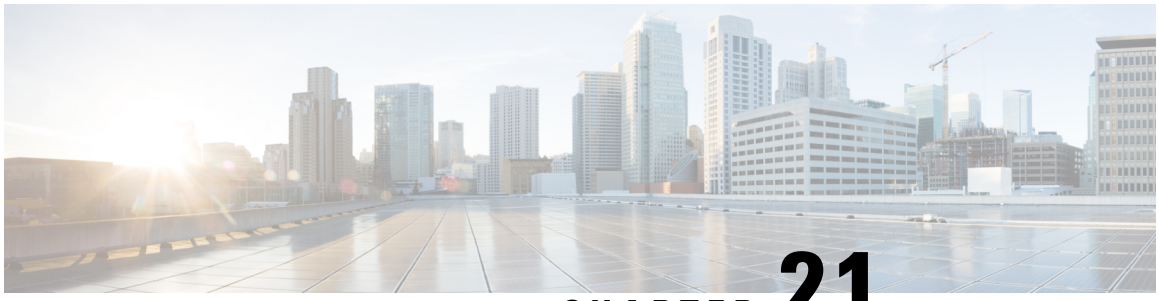
Delete Crosswork Data Gateways

You can delete a Crosswork Data Gateway to remove it completely. You can also **deactivate** a Crosswork Data Gateway, which retains the Crosswork Data Gateway information, but disables the Crosswork Data Gateway from sending network data to Crosswork Cloud.

Step 1 From the main window, click **Data Gateways**.

Step 2 Click on the Crosswork Data Gateway instance you want to delete.

Step 3 Click **Remove**. The Crosswork Data Gateway is removed.



CHAPTER 21

Send NetFlow Traffic to Multiple Destinations

Send NetFlow Traffic to Multiple Destinations

To save on resources, you may want to send all NetFlow data to one destination (for example, Crosswork Data Gateway) and have it forwarded to other devices. Crosswork Traffic Analysis allows you to forward NetFlow traffic to multiple IPv4 address destinations.

Note This feature is not supported if Crosswork Data Gateway was deployed using the OpenStack Platform (OSP).

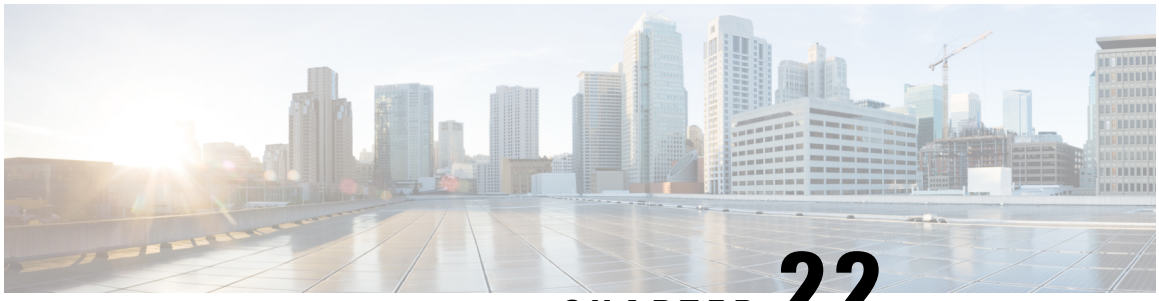
Step 1 From Crosswork Traffic Analysis, click **Configure > Flow Replication**.

Step 2 Click **Add**.

Step 3 Enter a global forwarding address. In addition to the global forwarding address, you can specify data gateways and devices.

Note Crosswork Traffic Analysis prioritizes the most granular configuration. For example, Crosswork Traffic Analysis will prioritize a device configuration over a data gateway configuration.

Step 4 Click **Save**.



CHAPTER 22

Configure Credentials

Create Credentials

You can specify credentials that are shared among a group of devices instead of manually entering this information for each device. Creating credentials allows multiple routers in a production environment to leverage a single login credential. This login credential may be defined in an external authentication service such as TACACS+ or RADIUS.

Step 1 In the main window, click **Configure > Credentials**.

Step 2 Click **Add Credential**.

Step 3 Enter a name for the credential, select the credential type, and complete the required fields.

Step 4 Click **Save**.

You can now apply this credential to devices you have added.

Edit Credentials

You can edit previously created credentials.

Step 1 In the main window, click **Configure > Credentials**.

Step 2 Click the name of the credential you want to edit.

Step 3 Click **Edit**.

Step 4 Make the required changes, then click **Save**.

Step 5 To link devices to this credential, click **Link Devices**.

The credential updates with the changes you made.

Link Devices to a Credential

You can link previously added devices to a credential group, which overwrites any previously assigned credential for the selected devices.

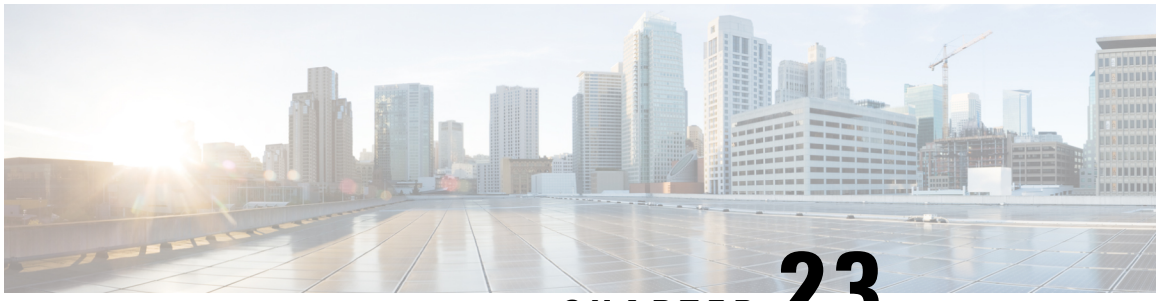
Step 1 In the main window, click **Configure** > **Credentials**.

Step 2 Click the name of the credential to which you want to link devices.

Devices for which you can link to the selected credential are displayed. If the specified credential isn't valid for the device, the device doesn't appear in the list.

Step 3 Click **Link Devices**.

Step 4 Select one or more devices to link to the credential, then click **Link**.



CHAPTER 23

Configure Device Groups

Create Device Groups

Creating device groups allows you to view and perform actions on a group of similar device types. A device can belong to only one device group.

Step 1 In the main window, click **Traffic Analysis > Configure > Device Groups**.

Step 2 Click **Add Device Group**.

Step 3 Enter a name for the device group and a description (optional).

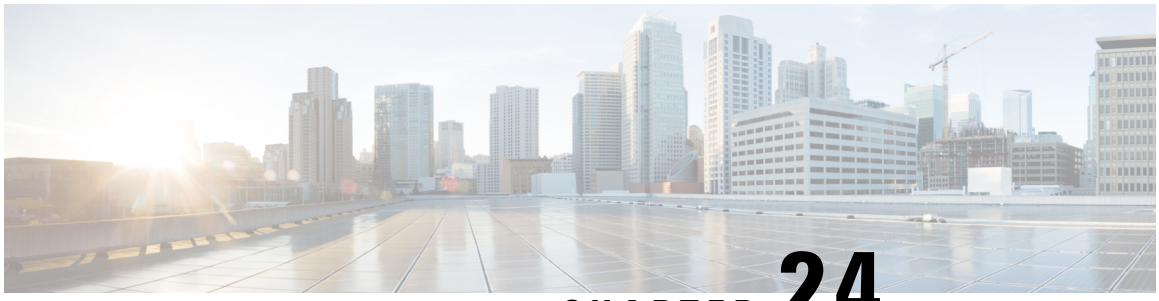
Step 4 Click **Save**.

Step 5 Click on the name of the device group you just created.

Step 6 To add devices to the device group, click **Link Devices**.

Step 7 Select the devices to add to the device group, then click **Link**.

A device can belong to one device group only. If any devices were previously added to a different device group, they are removed from the previous device group and added to the device group you selected.



CHAPTER 24

Configure Known Good Files

About Known Good Files

Crosswork Cloud Trust Insights automatically interprets and verifies the integrity of Known-Good-Values (KGVs) measurements from Cisco IOS XR routers. Crosswork Cloud Trust Insights also allows you to designate files that you have self-verified and qualified as having known good data.

Maintaining a list of known good files can help you ensure your devices are running the configuration you expect. See Add Known Good Files, on page 193 for more information.

Add Known Good Files

You can add known-good files to Crosswork Cloud Trust Insights so you can more easily locate and track them.

Step 1 In the main window, click **Trust Insights > Configure > Known Good Files**.

Step 2 Click **Add Files**.

Step 3 Select a device for which you want to save known-good files.

Step 4 To filter the device table, click **Add Filter**, enter the filter value, then click **Save**.

Step 5 After you select a device, click **Next**.

Crosswork Cloud Trust Insights displays a list of dossier collections for the device you specified.

Step 6 To find a dossier collection for a specific time frame, select a value from the **Timeframe** drop-down list.

An orange icon appears next to a dossier collection if the signing key changed on the device. Hover your cursor over an icon to display details about what changed.

Step 7 Select a dossier collection, then click **Next**.

Crosswork Cloud Trust Insights displays a list of files that have different KGVs than those already known (up to a maximum of 1,000 files).

Step 8 Select one or more files (up to a maximum of 1,000 files) that you want to designate as known-good files, then click **Submit**.

To add more than 1,000 files, repeat Step 8 as many times as needed.

The files you selected appear in the Known-Good files table.

Disable Known Good Files

You can disable any previously added known good files. If you aren't sure you want to delete a known good file, you can disable it to leave it in the table of Known Good Files, but the system will no longer recognize the known good files.

Step 1 In the main window, click **Trust Insights > Configure > Known Good Files**.

Step 2 Select one or more files, then click **Disable**.

Crosswork Cloud Trust Insights changes the state of the file to Disabled.

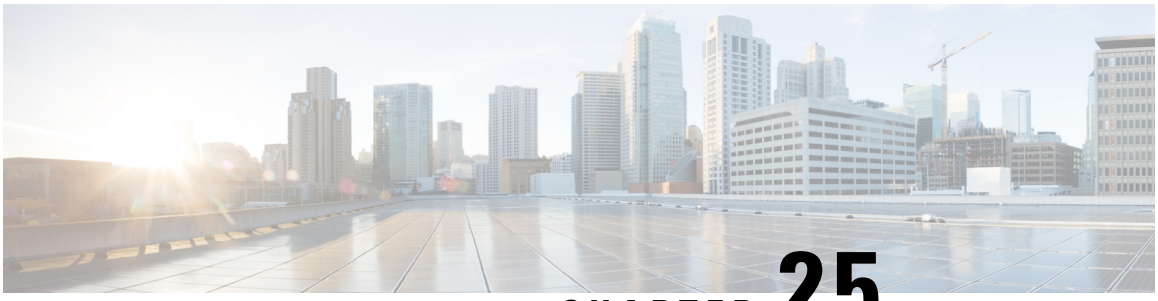
Delete Known Good Files

You can delete any previously added known good files. If you are unsure you want to delete a known good file, you can disable it. See Disable Known Good Files, on page 194 for more information.

Step 1 In the main window, click **Trust Insights > Configure > Known Good Files**.

Step 2 Select one or more files, then click **Remove**.

Step 3 To confirm that you want to remove the known good files, click **Remove**.



CHAPTER 25

Configure Reports

This section contains the following topics:

Configure ASN Routing Reports

The ASN Routing Report provides you with an easy to understand overview of any changes in route announcements and peering relationships for your Autonomous System. The ASN Routing Report captures the current state of an ASN, highlighting the *changes* from the time the last report instance was generated. The report runs daily, but can also be triggered on demand.

Crosswork Cloud collects and persists the following information for a selected ASN:

- Prefix BGP announcements
- ASN peers
- RIR, ROA, and RPSL prefix information

In addition to having a report instance sent to an endpoint, you can view its contents in the UI. For more information, see View Daily ASN Changes (ASN Routing Report), on page 36.

Important Notes

- A *report* refers to the report configuration. A *report instance* is the result of running a single instance of the report and contains the generated data.
- Each time a report instance is generated, the data is compared with the last generated report. The report instance includes a summary of changes from the last report. The last generated report can be either a daily report or a report generated manually.
- Individual report instances are stored for 30 days and then are deleted from the system.
- There is a limit of 30 total report instances that are saved per report configuration. The total report instances include both the daily reports and any reports generated on demand. For more information, see Generate Reports on Demand, on page 196.
- You can disable an ASN Routing Report (**External Routing Analytics > Configure > Reports**, then click the ASN Routing Report name and **Disable**) to prevent future generation of daily report instances. All previous report instances are still available unless they age out. However, if you delete an ASN

Routing Report (**External Routing Analytics > Configure > Reports**, then click the ASN Routing Report name and **Delete**), all previous report instances are also deleted.

- If you later unsubscribe from an ASN that is associated with a report configuration, no new report instances are generated. However, you will still be able to view prior report instances.
- Report instances age out and are deleted if a paid Crosswork Cloud subscription expires.
- You can also import or export report configurations. For more information, see Import and Export Configuration Files, on page 239.

Before you begin

You must subscribe to the ASN you are interested in before you configure a report. For more information, see Configure ASNs, on page 67.

Step 1 Confirm that you are subscribed to the ASN you are interested in.

Step 2 In the main menu, click **External Routing Analytics > Configure > Reports**.

Step 3 Click **Add**.

Step 4 Enter a report name in the **Name** field. When a report is generated, that report instance is named "<*report name*>-<*month*>-<*day*>-<*timestamp*>". For example, if you configure the report name as **ASN7100** and a report instance is generated on **July 4, 2021 at 10:00 UTC**, then the name given to that report instance is **ASN7100-Jul-04-10:00-UTC**.

Step 5 Enter the ASN and any tags.

Step 6 Click **Add Endpoint** and add the endpoint to which the daily report will be sent to.

Note S3 endpoint configuration is not supported.

Step 7 Click **Save**. The first report will be sent the next day to the endpoint you specified.

Generate Reports on Demand

In addition to the daily reports, you can generate a report on demand. This report will list the changes since the last generated report.

Before you begin

You must have an ASN Routing Report configured before generating a report manually. For more information, see Configure ASN Routing Reports, on page 195.

Step 1 In the main window, click **External Routing Analytics > Configure > Reports**.

Step 2 Click on a configured report name.

Step 3 Click **Generate**.

Step 4 Enter a unique report name for this particular report instance, then click **Generate Report**.

Note If a name is not entered, Crosswork Cloud generates a name automatically (<*configured-report-name*>-<*month*>-<*day*>-<*timestamp*>). For example, if the configured daily report name is **ASN7100** and a manual report instance is generated on **July 4, 2021 at 10:00 UTC**, then the name given to that report instance is **ASN7100-Jul-04-10:00-UTC**.

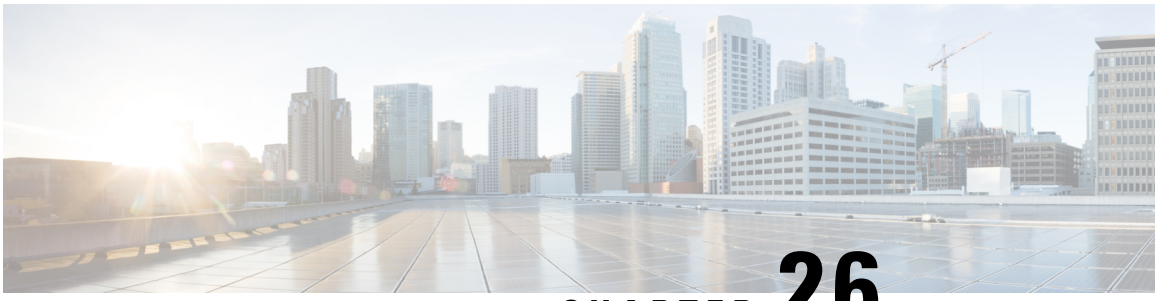
Step 5 Click **Go To Reports** and check to see that the Report Status is **In Progress**. The report is normally generated within 5 minutes. The **Reports** page automatically refreshes when the report is ready.

What to do next

View Daily ASN Changes (ASN Routing Report), on page 36

PART V

Use Crosswork External Analysis Tools



CHAPTER 26

Validate Route Origin Information

Validate Route Origin Information

The Route Origin Validation (ROV) tool compares ROA record information against the information received via BGP updates.

Step 1 In the main window, click **External Routing Analysis > Tools > Route Origin Validation**.

Step 2 Enter a single ASN to view associated prefix ROA records and click **View**. You can remove and add more ASNs later.

Step 3 From the Timeframe drop-down list, select a time period in which you want to view ROA records for.

Step 4 Edit, add, or remove filters. By default, the ROV Status with the **Invalid** option filter is enabled. This option lists all prefixes with ROA violations.

Example:

Click here to see an example of how to add ASNs, remove the ROV Status filter, and add the ROA Max Length filter.

Step 5 View the information in the ROV table.

Table 31: ROV Table Descriptions

Column/Field	Description
Prefix	The prefix that the ROA authorizes the ASN to advertise.
ROA Source	The organization that published the ROA. Examples: • American Registry for Internet Numbers (ARIN) • Internet Numbers Registry for Africa (AFRINIC) • Asia-Pacific Network Information Centre (APNIC) • Latin American and Caribbean Internet Addresses Registry (LACNIC) • Réseaux IP Européens (RIPE NCC)
ROA ASN	The AS number that is authorized by the ROA to originate the prefix.

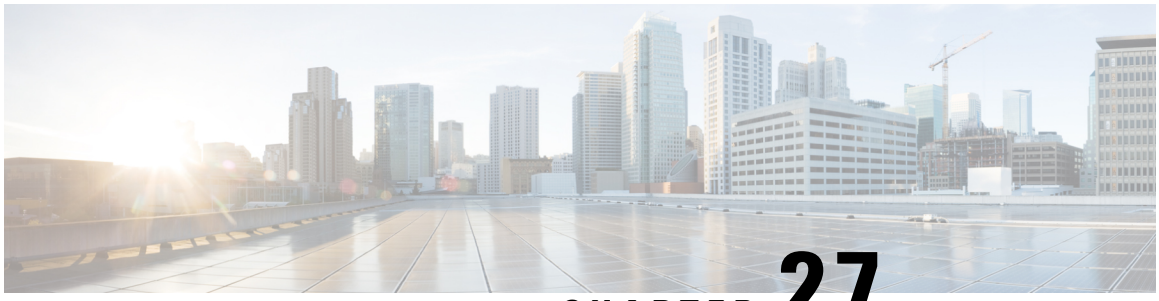
Column/Field	Description
Observed ASN	The origin ASN observed in the BGP update.
ROA Max Length	The maximum prefix length of the most specific IP prefix that the ROA authorizes the ASN to advertise.
Notes	If the ROV Status is **Invalid**, it will display the reason for the violation. Otherwise, it will display the date and time of the last ROA scan.
Last Updated	The date and time for which this ROA prefix data was last retrieved.
ROV Status	The status of the ROA which can be one of the following: • Valid—The ROA information matches the BGP update. • Invalid—The ROA information is different than the BGP update. • Unknown—This prefix does not have any matching ROAs.

Step 6 (Optional) Visualize the prefix path topology. Next to the prefix, click  .

Example

Figure 7: ROV Tool Example

Note If you are viewing the HTML version of this guide, click on the image to view it in full-size.



CHAPTER 27

View Prefix Path Topology

View Prefix Path Topology

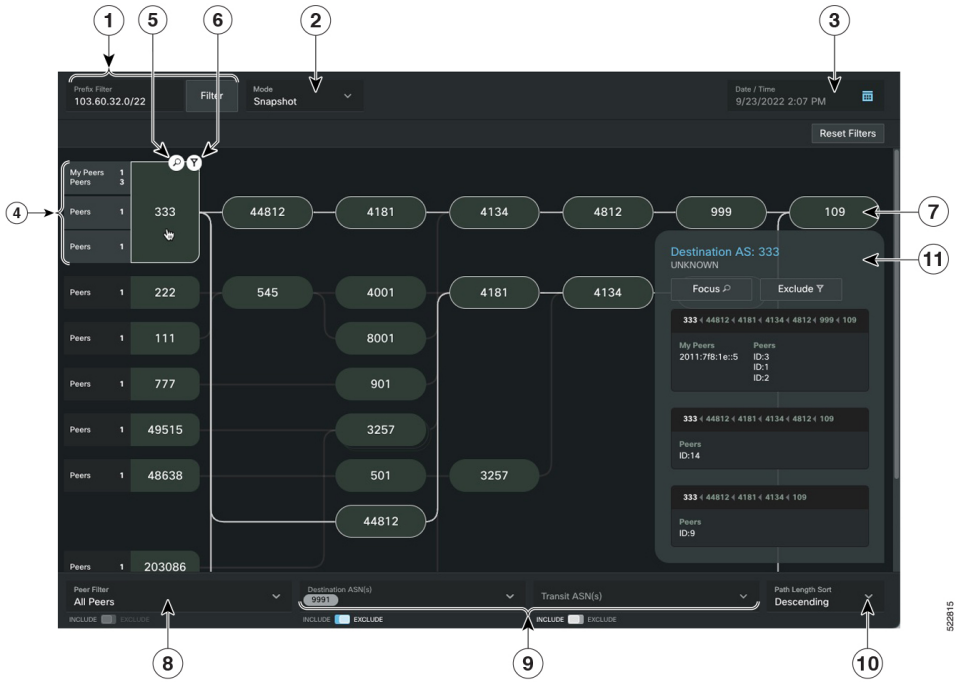
The Path Topology tool displays a summarized topology view of all peer, transit, and origin ASN that are advertised in AS paths for a prefix at a selected time. Visualizing prefix path topology can also help with decisions related to network planning by identifying AS paths that meet a certain criteria so that, for example, the paths can be reprioritized. When My Peers are defined (**Configure > Peers > Add Peers**), the visual aid offers a quick overview and ability to easily identify and address BGP misconfigurations for the peers you are responsible for. Another added benefit, is the ease of sharing filtered views because of a stateful URL. Any type of sort or filter applied to your topology view is assigned a specific URL and can be shared.

Step 1 In the main window, click **External Routing Analysis > Tools > Path Topology**.

Step 2 Enter a prefix and click **View**. The page displays the path topology filtered by the prefix you entered and, by default, the current time. The path is displayed from ASN destination to origin (left to right). As you highlight individual ASNs, the associated paths are highlighted.

Example

Figure 8: Path Topology

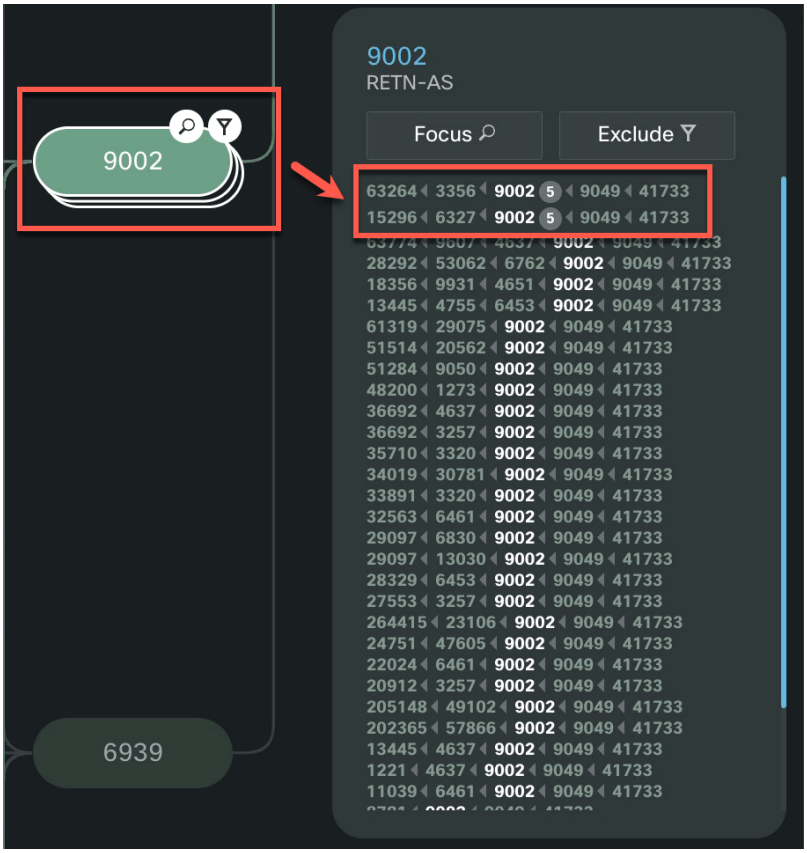


Note If you are viewing the HTML version of this guide, click on the image to view it in full-size.

Callout No.	Description
1	Path topology is filtered based on what prefix is entered here. Each time you enter a new prefix, click **Filter** to display the results
2	The **Snapshot** mode displays the ASN path topology for the displayed time in the **Date/Time** field. The **Time Comparison** mode allows you to compare changes between two timestamps. When this mode is selected, select the Baseline and Comparison dates. The Path Topology will display and indicate path, node, and peer changes that have occurred since the baseline date to the comparison date. For more information, see Compare Path Topology Changes, on page 206.
3	Displays the prefix path topology view at the selected date and time. Click this area to configure other dates and times you want to view.
4	Summarizes the number of peers that advertise a given path with the same destination ASN. In this example, there are 3 paths. To find more details about the peers and paths click the destination ASN.

Callout No.	Description
5	Click to visually focus on paths that only include the selected ASN. All other paths, where this ASN is not included, will be removed from the topology.
6	Click to visually exclude paths that include the selected ASN. All paths that include this ASN will be removed from the topology.
7	The origin ASN.
8	Allows you to choose whether to only view the topology for AS paths advertised by peers that belong to your organization (My Peers) or for those advertised by all peers. The My Peers view allows you to easily view what AS paths your peers are advertising for a prefix which can help with routing configuration decisions.
9	Allows you to select multiple destination or transit ASNs to visually exclude or focus on in the path topology.
10	Allows you to visually sort paths according to the number of hops (path length) either in descending or ascending order.
11	This window appears when an ASN is clicked on. It displays the ASN name and raw path data (indicating path stuffing (also known as ASN path prepending) count where applicable, see ASN Path Stuffing Example). If a destination ASN is selected, it also displays the peers advertising this path. From this window, you can also do the following: • Choose to visually focus or exclude the ASN from the path topology. • Click the ASN link to display the ASN Details page where you can get more ASN information.

Figure 9: ASN Path Stuffing (ASN Path Prepending) Example



A stacked ASN node indicates that the ASN has been inserted into a path multiple times.

Compare Path Topology Changes

The Path Topology tool provides you insight to help troubleshoot issues that might have occurred with routing traffic for the prefix during a specified time (for example, bandwidth or latency issues due to AS path changes). Suppose a network outage occurs and you want to investigate what changed. You can view the changes in the ASN node topology and peer path by comparing the topology before and after the time at which the problem was observed.

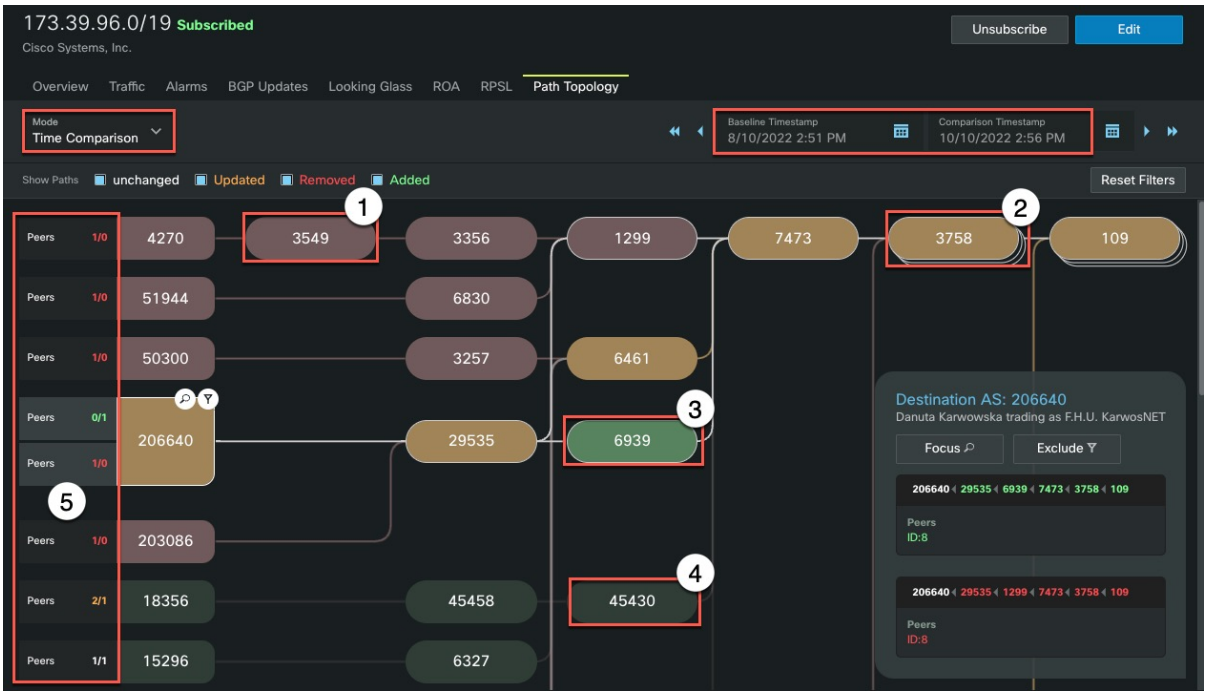
To view path topology changes:

Step 1 In the **Path Topology** window, select **Time Comparison** from the **Mode** drop-down list.

Step 2 Click the **Baseline Timestamp** field and select the date and time you want to use as a reference for path topology changes. You can use the single arrow or double arrows to adjust the time to advance or move back 1 minute or 5 minutes.

Step 3 Click the **Comparison Timestamp** field and select the date and time you want to use to compare with the baseline timestamp.

In Time Comparison mode, topology changes are highlighted using different ASN node colors and path changes are highlighted using different peer text colors (showing peer In counts/IDs). See the following example and descriptions of what each color might indicate:



Note Click the image to view it in full-size.

Callout No.	Description
AS Node Changes	
1	**Removed AS Node (red)**—Indicates that the advertised AS paths that had the AS Node at that hop in them have been withdrawn after the baseline timestamp.

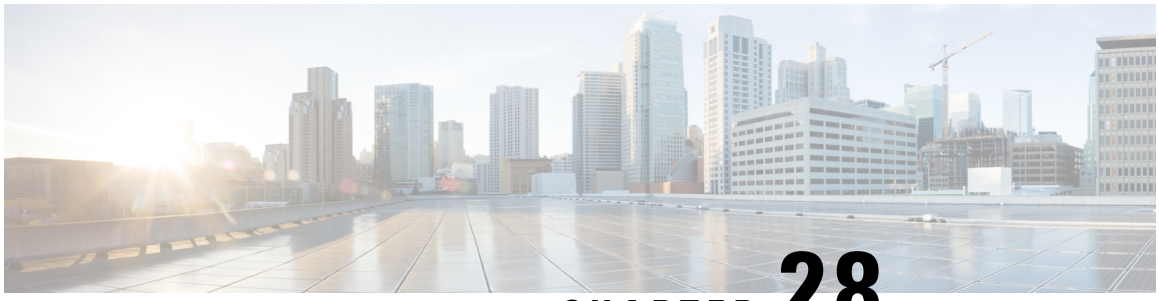
2	**Updated AS Node (yellow/brown)**—Indicates that the ASN at that hop was present in one or more other AS paths at both the timestamps, however, there were some changes:
	• **Path Count Changes**—Some new AS paths advertised have this AS node/hop and/or some old AS paths advertised with the AS node/hop have been withdrawn some time after the baseline timestamp
	• **Path Stuffing Changes**—This AS node/hop was either:
	  • Stuffed in one or more AS paths before and not stuffed now
	  • Stuffed in one or more AS paths now and not stuffed before
	  • Stuffed in one or more AS paths now and before, but the count changed

3	**Added AS Node (green)**—Indicates that the AS Node at that hop is present in one or more new AS paths advertised after the baseline timestamp, but was not previously present during the baseline time.

Callout No.	Description
4	**Unchanged AS Node (dark green/gray)**—Indicates that the AS Node at that hop is present in one or more other AS paths advertised at both timestamps.
Peer Count Changes The change in the count of peers advertising a path is annotated with text next to the peer ASN that terminated that AS path. The syntax of the peer change is ***before_peer_count*/*after_peer_count***.	
5	• **0/*n* (green)**—Indicates that no peers were advertising this path at the baseline time but ***n*** peers were advertising the path at the comparison time • ***n*/0 (red)**—Indicates that ***n*** peers were advertising this path at the baseline time, but peers were no longer advertising the path at the comparison time. • ***b*/*a* (yellow)**—Indicates that ***b*** peers were advertising this path at the baseline time and ***a*** peers were advertising the path at the comparison time • ***n*/*n* (white):** —Indicates that there were no changes in the number of peers advertising the path after the baseline time, but before or equal to the comparison time.

PART VI

Use Crosswork Traffic Analysis Tools



CHAPTER 28

Optimize Interface Utilization

Optimize Interface Utilization

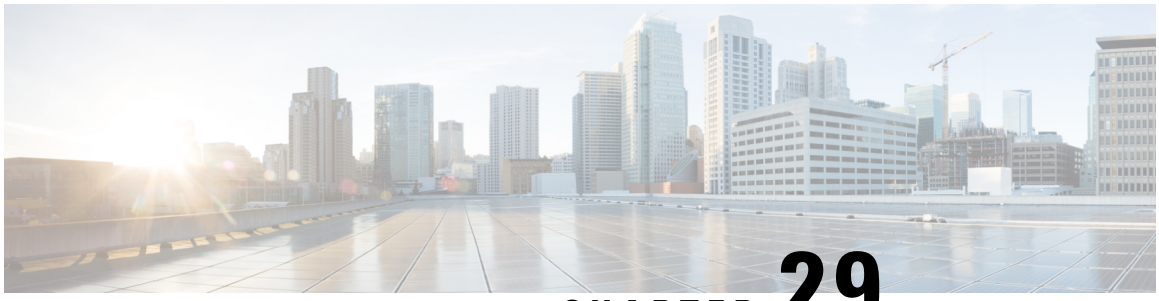
You can optimize your network by diverting high utilization traffic to other interfaces within a device group. The Recommendations tool analyzes network edge interfaces that have a *transmitted* utilization of over 80% (for example, if an edge interface has a transmitted utilization of 20% and a received utilization of 90%, the edge interface is not considered as part of the analysis.). The tool provides you with a suggested list of prefixes where traffic from overutilized edge interfaces can be diverted to underutilized edge interfaces to normalize overall utilization. The utilization projections are estimates based on the original traffic flow. You can use these recommendations to determine how to best balance your network traffic load.

Step 1 In the main window, click **Traffic Analysis > Tools > Recommendations**.

Step 2 From the **Device Group** drop-down list, select a device group to view the prospective prefixes contained in that device group only. The page displays the following information:

- Prefix, transmit traffic rate, and interface utilization status during the duration selected in the **Timeframe** drop-down list.
- Alternate interfaces that can be used to offload traffic and alleviate congestion.
- Projected interface utilization if the recommendations are manually configured on the devices within the device group. These projections are estimations based on the original traffic flow.

Step 3 To exclude prefixes from being analyzed, click **Ignore Prefix**. To add the prefix back, navigate to the **Ignored** tab and click **Resume Tracking**.



CHAPTER 29

Traffic Drilldown

Traffic Drilldown

The Traffic Drilldown tool allows you to easily view interface capacity and what traffic sources are contributing to it.

Step 1 In the main window, click **Traffic Analysis > Tools > Traffic Drilldown**.

Step 2 Click one of the following options:

a) **Device Centric**—Displays a list of devices, from which you can view device information including device utilization, device group, capacity, TX/RX SNMP traffic, and tags.

Note To filter the device **Utilization** column, click **Edit Filter** and slide either end of the 0 to 100 scale to specify the utilization percentage range you want displayed. Crosswork Cloud Traffic Analysis determines utilization by taking the *highest* utilization of all the interfaces on a device. To view individual interface utilization, click the device name. The following values are available:

- Balanced—Utilization on all interfaces is less than 50%.
- Skewed—The highest utilization on any interface is equal to or more than 50%, but less than 80%.
- Unbalanced—At least one of the interfaces has utilization that is above 80%.

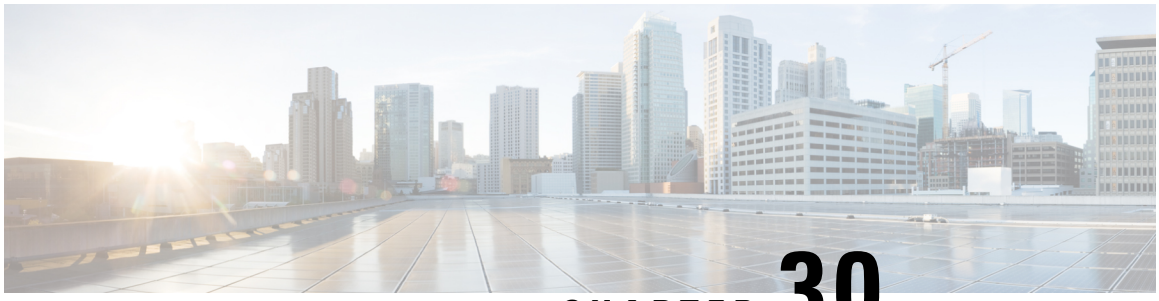
1. To view further device interface details, click on a device name. A list of interfaces for the device appears and displays individual interface information.
2. To view interface ASN or Prefix information, click on an interface and select the appropriate option from the **Breakdown** filter list.

b) **Prefix Centric**—Displays a list of prefixes, from which you can view tags, TX/RX Netflow traffic, and total traffic.

1. To view prefix device details, click on a prefix. The device information appears.
2. To view further device interface details, click on the device name.

a) **ASN Centric**—Displays a list of ASNs, from which you can view prefixes, TX/RX Netflow traffic, and total traffic.

1. To view prefix device details, click on a prefix. The device information appears.
2. To view further device interface details, click on the device name.



CHAPTER 30

Peer Prospecting

Peer Prospecting Overview

Note This feature is for Crosswork Traffic Analysis only.

The Peer Prospecting tool shows you on which peer ASNs large amounts of traffic are being transmitted and received. It helps you select a current peer and quickly see other peers to which you could move traffic. For example, if a service provider charges more money for its traffic throughput, you might want to move traffic away from its peers to another peer that is less expensive. Peer Prospecting can help you identify other peers to which you can move your traffic.

Note You must have an Advanced license to use this feature. Contact sales@crosswork.cisco.com for more information.

Find Recommended Peers

You can view a list of ASNs that you are not currently peered with, but to which you are sending a significant amount of traffic. This can help you understand to which ASNs you should be peered with but are not.

Note You must have an Advanced license to use this feature. Contact sales@crosswork.cisco.com for more information.

Step 1 In the main window, click **Traffic Analysis > Tools > Peer Prospecting**.

By default, the **Non-Peers** option is selected which indicates that the table contains all ASNs that are not currently peers.

Step 2 In the Filter By field, select one of the following options:

- **Device Group**—Click **Device Group**, then select a device group from the drop-down list to view the prospective peers contained in that device group only.
- **Device**—Click **Device**, then select a device from the drop-down list to view the prospective peers of that device type only.

Step 3 Select one of the following Traffic Aggregation values to display:

- **Both**—Aggregates RX, TX, and total data for all traffic for the specific ASN.
- **Transit**—Aggregates RX, TX, and total data when the ASN is not the source or destination of the traffic but rather an intermediary peer somewhere along the path. Looking at transit data can help you determine, for example, if peering with a specific ASN can shorten your traffic path.
- **To/From**—Aggregates Rx, Tx, and total data for source and destination ASNs.

Step 4 To view data for a specific time period, select a time from the **Timeframe** drop-down list.

The table contains a list of ASNs which can be prospective peers. By default, the table is organized by descending total traffic data.

Step 5 Click **Ignore** to hide an ASN from the list of prospective peers. See Ignore Recommended Peers, on page 217 for more information.

Step 6 Click on the ASN in the **Prospect** column to view details about that ASN.

Optimize Peers

You can view the ASNs to which you are peered and determine if there are other peers to which you can move traffic in order to optimize your network.

Note You must have an Advanced license to use this feature. Contact sales@crosswork.cisco.com for more information.

Step 1 In the main window, click **Traffic Analysis > Tools > Peer Prospecting**.

Step 2 Click **Optimize Peer**, then enter the Peer ASN for which you want to optimize.

Step 3 In the Filter By field, select one of the following options:

- **Device Group**—Click **Device Group**, then select a device group from the drop-down list to view the prospective peers contained in that device group only.

- **Device**—Click **Device**, then select a device from the drop-down list to view the prospective peers of that device type only.

Step 4 Select one of the following Traffic Aggregation values to display:

- **Both**—Aggregates RX, TX, and total data for all traffic for the specific ASN.
- **Transit**—Aggregates RX, TX, and total data when the ASN is not the source or destination of the traffic but rather an intermediary peer somewhere along the path. Looking at transit data can help you determine, for example, if peering with a specific ASN can shorten your traffic path.
- **To/From**—Aggregates RX, TX, and total data for source and destination ASNs.

Step 5 To view data for a specific time period, select a time from the **Timeframe** drop-down list.

The table contains a list of ASNs which can be prospective peers. By default, the table is organized by descending total traffic data.

Step 6 Click **Ignore** to hide an ASN from the list of prospective peers.

Step 7 Click on the ASN in the **Prospect** column to view details about that ASN.

Ignore Recommended Peers

You can ignore any peers that are recommended so they do not show up under the list of Recommendations on the Peer Prospecting page. This is helpful if you know that you cannot or should not peer with an ASN that is listed as a prospective peer.

Note You must have an Advanced license to use this feature. Contact sales@crosswork.cisco.com for more information.

Step 1 In the main window, click **Traffic Analysis > Tools > Peer Prospecting**.

By default, the **Recommendations** option is selected which indicates that the table contains all recommended ASNs that are not currently peers.

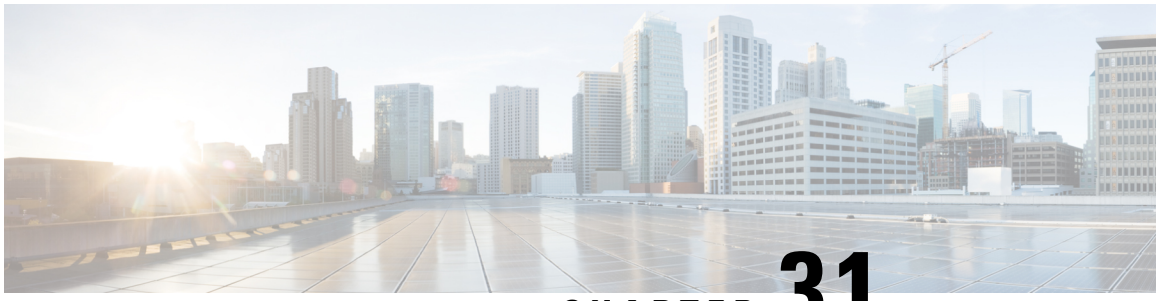
Step 2 In the table, click **IGNORE** under the Action column for any ASN you want to ignore.

The ASN is removed from the table.

Step 3 Click **Ignored** at the top of the page to view the list of prospective ASNs that you selected to ignore.

Step 4 To unignore an ASN, click **INCLUDE** under the Action column for any ASN that you want to move to the list of recommended prospective ASNs.

The ASN is removed from the Ignored table and appears on the Recommendations table.



CHAPTER 31

Compare Traffic

Compare Traffic

You can compare traffic between like objects such as ASNs, prefixes, devices, and interfaces. Viewing a quick visual comparison of traffic can help you see differences in traffic between the objects.

Step 1 In the main window, click **Traffic Analysis > Tools > Traffic Comparison**.

Step 2 From the **Object** drop-down list, select the object type for which you want to compare traffic.

Step 3 From the **Time** drop-down list, select the time frame for which you want to compare traffic.

The **Updated** box indicates the time for which the traffic data was last updated. Click the refresh icon to update the traffic information.

Step 4 If you selected **ASNs** in Step 2, select one of the following traffic values to display:

- **Transit**—Aggregates Rx, Tx, and total data when the ASN is not the source or destination of the traffic but rather an intermediary peer somewhere along the path. Looking at transit data can help you determine, for example, if peering with a specific ASN can shorten your traffic path.
- **Both**—Aggregates Rx, Tx, and total data for all traffic for the specific ASN.
- **To/From**—Aggregates Rx, Tx, and total data for source and destination ASNs.

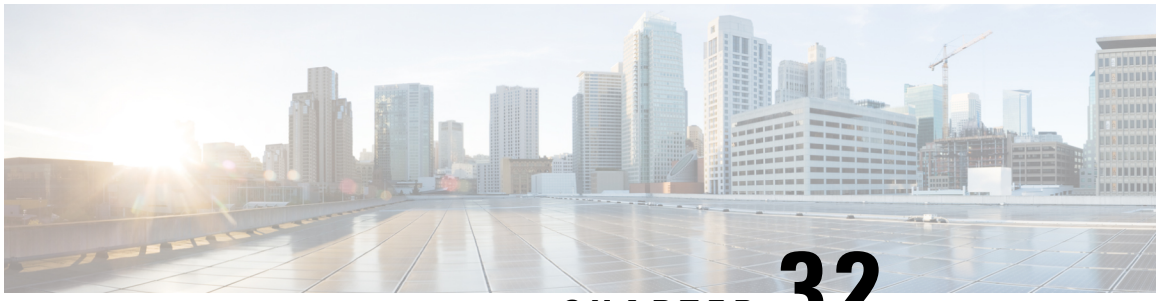
Step 5 Click **Add** to select the objects that you want to compare. You can select objects that correspond to the object type you selected in Step 2.

Separate each object with a comma.

Step 6 Click **Save**.

PART VII

Use Crosswork Trust Insights Tools



CHAPTER 32

Compare Devices

About Device Comparison

Crosswork Cloud Trust Insights allows you to quickly compare devices to view differences in their running software.

Compare Devices

You can easily compare devices to view their differences.

Step 1 In the main window, click **Trust Insights > Device Comparison**.

Step 2 Select the device to use as your baseline on which to compare other devices.

Crosswork Cloud Trust Insights displays a table described below that lists all other devices and their differences as compared to the baseline device you selected.

Table 32: Device Comparison Field Descriptions

Field	Description
Deviations	Number of differences, or deviations, the device has as compared to the baseline device.
Device	Name of the device being compared to the baseline device.
Location	Location of the device.
Model	Model of the device.
Version	Software version running on the device.

Field	Description
Software Differences (FIRST 500)	A list of the software differences the device has as compared to the baseline device. If there are more than 500 software differences, only the first 500 are displayed. Click on any blue hyperlink to view the specific changes you need to make in order to have the selected device match the baseline device.

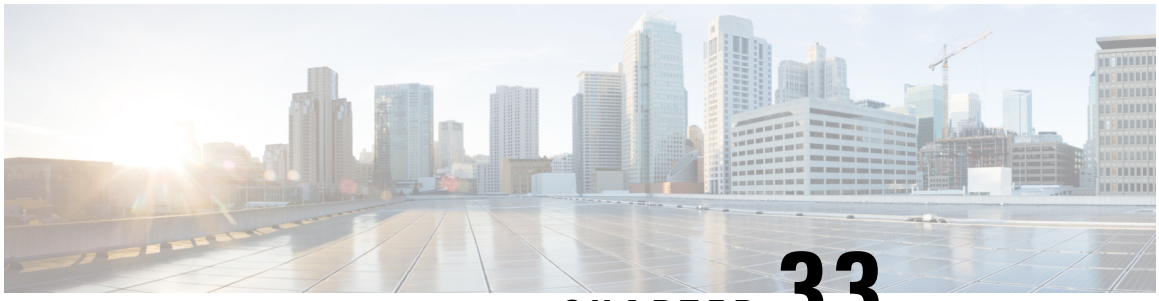
By default, the table is sorted according to the number of differences, or deviations, each device has as compared to the baseline device you selected.

Step 3 To search for a device, enter characters in the **Quick Search** field.

Crosswork Cloud Trust Insights displays only the devices that match the search criteria you entered.

Step 4 Click **View Punchlist** to view a list of the devices that differ from the baseline device and a summary of the differences.

Step 5 Click **Export CSV** to export the list to a CSV file.



CHAPTER 33

Find Packages

Find Packages

Crosswork Cloud Trust Insights helps you quickly find installed SMU packages, which can be helpful if you want to replace a version of software or update an SMU to fix a security vulnerability.

Step 1 In the main window, click **Trust Insights > Find Package**.

Step 2 In the View field, select one of the following options:

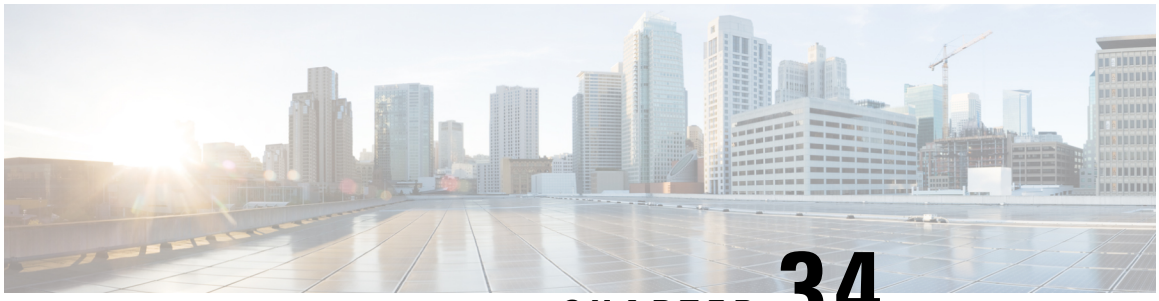
- **Search**—Searches for all packages.
- **Committed But Not Activated**—Searches for packages that are committed but not activated.

Step 3 Enter at least 3 characters on which to search.

Step 4 Select one of the following options:

- **Include**—Searches for packages that include the characters you entered.
- **Exclude**—Searches for packages that do not include the characters you entered.

Crosswork Cloud Trust Insights displays the packages that match the criteria you specified.



CHAPTER 34

Find Hardware

Find Hardware

Crosswork Cloud Trust Insights helps you quickly find hardware, which can be helpful if you want to view specific information about our hardware.

Step 1 In the main window, click **Tools > Find Hardware**

Step 2 Click **Add Filter**.

Step 3 In the Filter field, select the attribute for which you want to search.

Step 4 In the Filter Value field, enter the value for which you want to search.

Step 5 Click **Save**.

The table displays all the hardware that matches the search attributes you entered.

View Hardware Changes

Crosswork Cloud Trust Insights provides an easy way to view hardware changes reflected by your devices in the last received trust dossier. Using Crosswork Cloud Trust Insights, you can detect and track changes to production systems throughout their operational lifecycle.

Step 1 In the Crosswork Cloud Trust Insights main window, click **Devices**.

Trust Insights displays a list of previously added devices. See Add Devices, on page 164 for more information.

Step 2 Click on the device name for which you want to view hardware changes.

Step 3 Click the **Changes** tab.

Crosswork Cloud Trust Insights highlights observed events over a historical timeline for the device you selected.

Step 4 To view changes for a specified time, click an option next to **Timeframe**.

View Hardware Inventory

Crosswork Cloud Trust Insights provides an easy way to view hardware inventory reflected by your devices in the last received trust dossier.

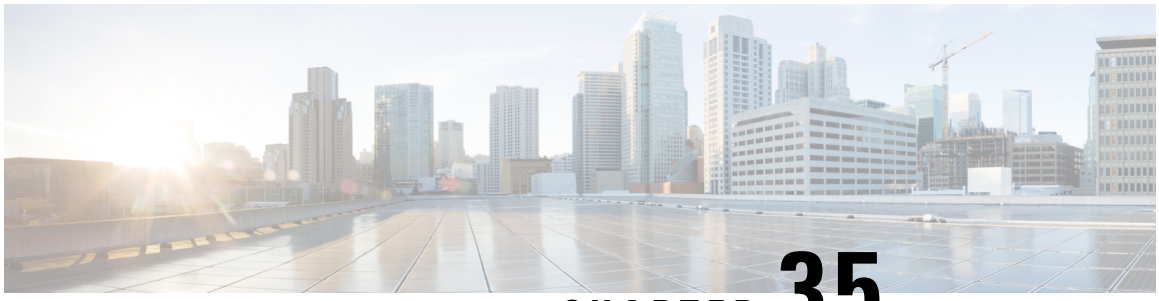
Step 1 In the Crosswork Cloud Trust Insights main window, click **Devices**.

Trust Insights displays a list of previously added devices. See Add Devices, on page 164 for more information.

Step 2 Click on the device name for which you want to view hardware information.

By default, **Hardware** is selected and hardware information is displayed.

Step 3 Click on a name in **Node** column to display specific information about that node. Crosswork Cloud Trust Insights displays a history of where this individual component was previously observed. The hardware component history track individual hardware FRUs, based on their confirmed serial number, across systems over time.



CHAPTER 35

Find Files

Find Files

Crosswork Cloud Trust Insights helps you quickly find files. For example,this can be helpful in cases where you are verifying checksums or find an unknown file (SHA-256 checksum) and you want to see if the files are located anywhere in your network infrastructure. You would then be able to find the hosts the file was found on, when it was first found, and whether it is still present.

Step 1 In the main window, click **Trust Insights > Find Files**.

Step 2 To use either a partial hash, filename, or path to find the file, click **Find By File**.

a) From the Filter Type drop down list, select one of the following:

- **Hash**—Enter at least 3 characters of the hash value. The hash value is typically a string of hexadecimal characters.
- **File and Path**—Enter the path with the filename.

b) To begin the search, click **Search**.

Step 3 To find files by device type and additional filters, click **Find By Device Type**.

a) From the Device Type drop down list, select one of the devices.

b) Click **Add Filter** and select the type of filter, the filter value, and whether to include or exclude, the value from the result. The following filter types are available:

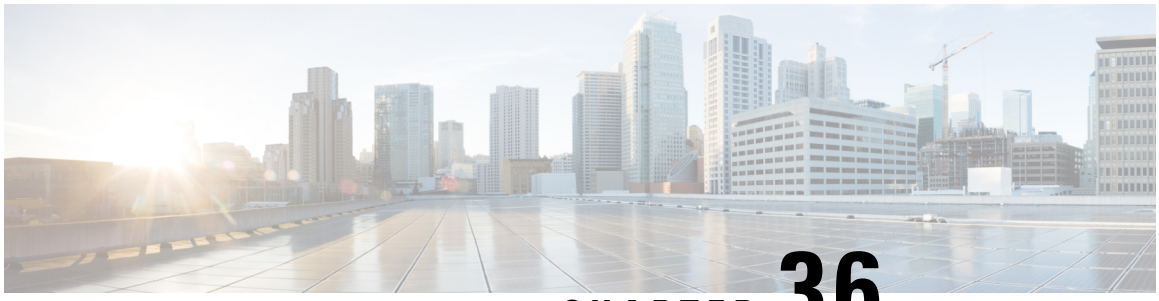
- Package Name
- Device Name
- Tag
- Mismatch
- OS Version
- Path

Note
- **Include**—Searches for files that include the values you entered.
- **Exclude**—Searches for files that do not include the values you entered.

c) Click **Add**.
d) Click **Add Filter** to add additional filters.

PART VIII

Administrative Tasks



CHAPTER 36

Manage Users

Add Users

You must have admin privileges to add users.

Users must have a Cisco.com account because they must enter their Cisco.com username and password to log in.

Step 1 In the main window, click **Settings** in the bottom-left corner.

Step 2 Click **Users**.

Note The **Users** menu appears for users with Admin privileges only.

Step 3 Click **Add User**.

Step 4 Specify whether the user is **Enabled** (default) or **Disabled**.

Disabled users can't log in.

Step 5 Enter the user's email address specified in their Cisco.com user profile.

To add multiple users, separate each email address with a space, a comma (,) or a semicolon (;).

Step 6 Select the user's role, which determines what tasks they can perform. See User Roles, on page 234 for more information.

Step 7 The Provider field displays the same provider to which you, as the Admin, belong.

Step 8 Click **Save**.

User Roles

A user role defines the permissions users have to perform tasks. The following table describes the user roles and tasks for which they have permissions.

Table 33: User Role and Permission Descriptions

User Role	Permissions
Admin	Can perform all tasks including adding and editing users.
Read/write	Can perform all tasks except adding and editing users.
Read Only	Can read all data and modify their user settings only.

Change User Permissions

You modify a user's role to determine which tasks that user can perform. You must have admin privileges to modify user permissions.

Step 1 In the main window, click **Settings** in the bottom-left corner.

Step 2 Click **Users**.

Note The **Users** menu appears for users with Admin privileges only.

Step 3 Check the checkbox of the user whose permissions you want to change. You can check multiple users at the same time.

Step 4 Click **Edit**.

Step 5 To suspend a user's permissions, check the first **Edit Value** checkbox and select **Disabled** from the drop-down **State** list. The user can't log in until you change the status to **Enabled**.

Step 6 To change a user's role, check the second **Edit Value** checkbox and select a role from the drop-down **Role** list. See User Roles, on page 234 for more information about what tasks each role can perform.

Step 7 Click **Next**.

Step 8 Review the changes and click **Save**.

View User Profiles

You can view a user profile to see their role, status, and last login. You must have admin privileges to view user profiles.

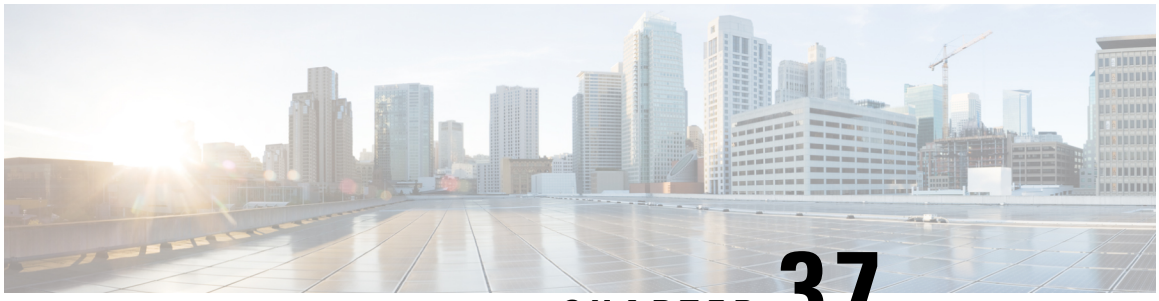
Step 1 In the main window, click **Settings** in the bottom-left corner.

Step 2 Click **Users**.

Note The **Users** menu appears for users with Admin privileges only.

A table lists all the users and their role, status, and last login.

Step 3 To modify a user's access, click on the user email address. See Change User Permissions, on page 234 for more information.



CHAPTER 37

Manage Licensing

Activate a Subscription or Trial

You can activate a subscription in Crosswork Cloud.

Note You must have admin privileges to activate a subscription. See User Roles, on page 234 for more information.

Before you begin

To activate a subscription, you must have one or more subscription IDs which are given or emailed to you after purchasing Crosswork Cloud.

Step 1 In the main window, click in the bottom-left corner.

Step 2 Click **Licensing**.

Step 3 To activate a subscription:

a) Click **Entitlement > External Route Analysis**, **Trust Insights**, or **Traffic Analysis** tab.

b) Click **Claim Subscription** and enter your subscription IDs in the text box. To add multiple subscription IDs, separate each ID with a comma or enter each ID on a new line.

Step 4 To request a Crosswork Cloud product trial version:

a) Click the **Trials** tab.

b) Click **Request** next to the Crosswork Cloud product you would like to try. Accept the terms and click **Start Trial**.

Modify Organization Name

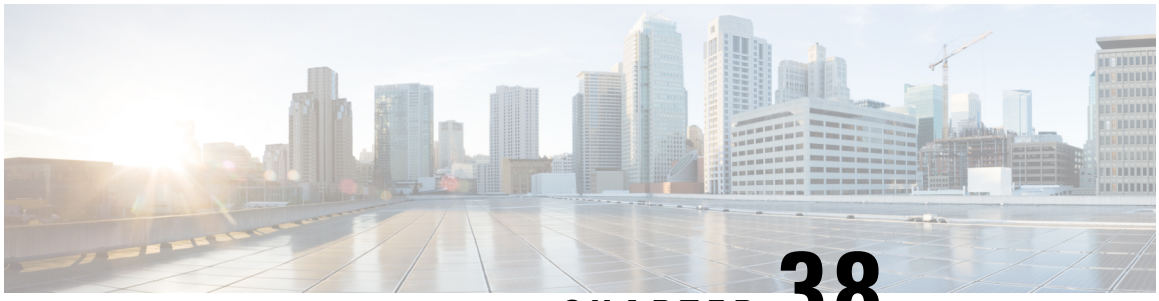
You can modify the name of your organization.

Step 1 In the main window, click  in the bottom-left corner.

Step 2 Click **Licensing**.

Step 3 Click **Edit**.

Step 4 Enter a new organization name, then click **Save**.



CHAPTER 38

Import and Export Configuration Files

Upload a Configuration File

You can upload a configuration file that contains prefixes, ASNs, policies, and notification settings. When you upload a configuration file, it overwrites any existing data of the same type. For example, if you previously added prefixes and your configuration file contains empty prefixes, your existing prefixes are deleted.

Note Before making significant configuration changes, such as uploading a new configuration file, we recommend you download and save your existing configuration file to serve as a backup file. See Download a Configuration File, on page 240 for more information.

Step 1 From the main window, click **Settings** in the bottom-left corner.

Step 2 Click **Import/Export**.

Step 3 Click **Upload Config File** to navigate to the location of your JSON configuration file.

You can also download a sample JSON configuration file by clicking the specified link.

Step 4 Click **Next**.

Step 5 Navigate to the appropriate tab to preview the contents of your configuration file and view what information will be added and deleted.

Step 6 Click **Submit**.

Download a Configuration File

Before you begin

Before you make any significant configuration changes, we recommend you download and save your configuration file to serve as a backup file.

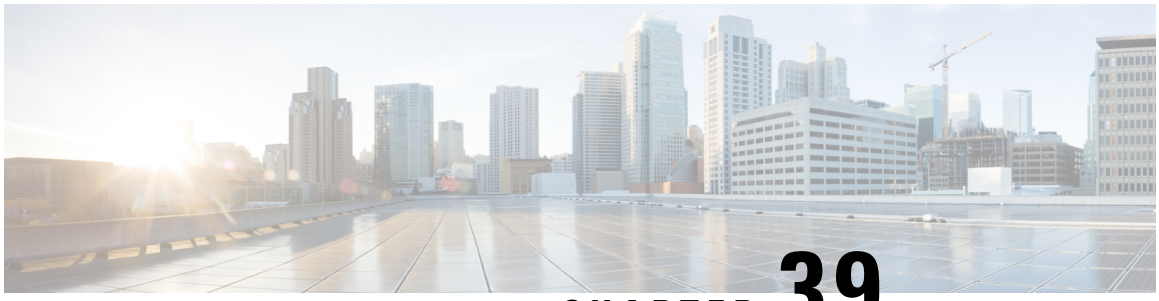
Note Due to significant changes and enhancements, if you downloaded a configuration file prior to November 12, 2019, you must download a new configuration file. Configuration files downloaded before November 12, 2019 contain significant differences and cannot be uploaded.

Step 1 From the main window, click **Settings** in the bottom-left corner.

Step 2 Click **Import/Export**.

Step 3 Click **Export Configuration** to download your JSON configuration file.

Your configuration file (.json) is saved.



CHAPTER 39

View a List of Actions Performed

View a List of Actions Performed

You can view a list of all actions performed in the Crosswork Cloud applications. This can you help you better understand what changes were made, who made the changes, and the date and time the changes were made.

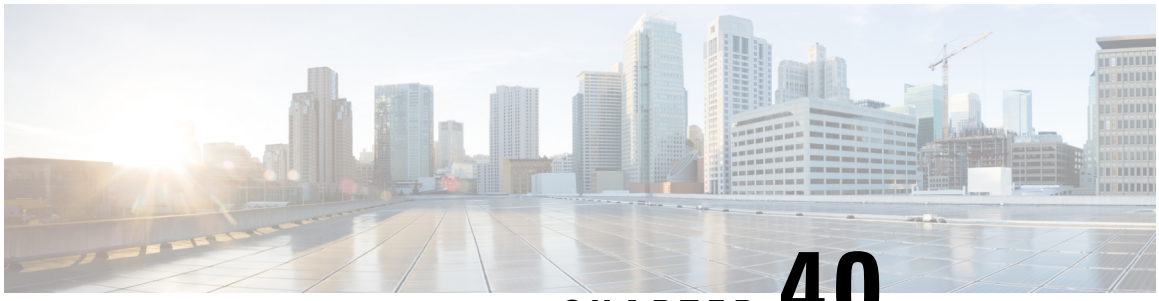
Step 1 In the main window, click the **Activity Log** icon ( ) in the bottom left corner.

By default, all changes are shown.

Step 2 To view activity during a specified time period, select a time period from the **Timeframe** drop-down list.

Step 3 To view specific changes, click on one of the following choices:

- ASNs
- Credentials
- Data Gateways
- Devices
- Device Groups
- Endpoints
- Interfaces
- Peers
- Policies
- Prefixes
- Reports
- Users



CHAPTER 40

Get Product Help and Support

Open a Support Case

Crosswork Cloud allows you to open a support case from within the product.

From the main window, click > **Support** > **Open a Support Case**. A new browser window opens displaying the Support Case Manager.

Submit Product Feedback

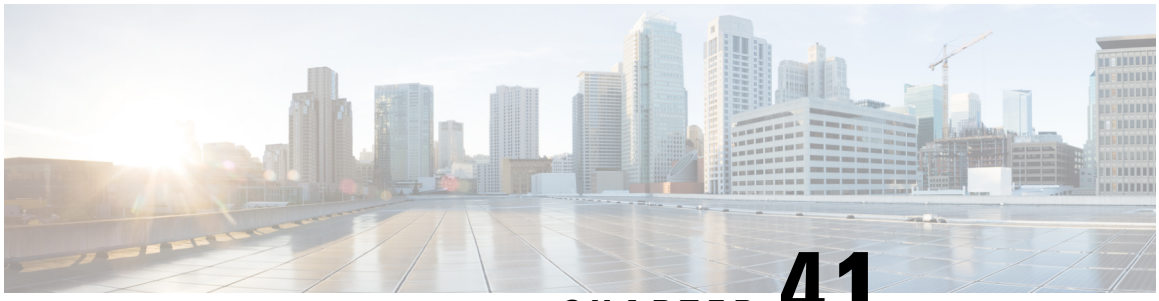
We welcome your feedback on our Crosswork Cloud products and encourage you to let us know about how we're doing.

From the main window, click > **Support** > **Product Feedback**.

Access the Cisco Community Forum

You can access the Cisco Community Forum to access FAQs, product announcements, and other product information. The forum also allows you to learn, share, and collaborate with other product users.

From the main window, click > **Support** > **Community Forum**. A new browser window opens with the Crosswork Cloud forum.



CHAPTER 41

Crosswork Cloud APIs

Overview of the Crosswork Cloud APIs

Crosswork Cloud APIs are for programmers who want to use the APIs with their network management and operations applications.

The Crosswork Cloud Network Insights API allows you to perform configuration tasks such as subscribing to prefixes or ASNs, configuring notification endpoints, and specifying conditions under which an alarm is triggered. The Crosswork Cloud Traffic Analysis API retrieves traffic statistics.

API Help and Documentation

You must be logged into Crosswork Cloud to access the Crosswork Cloud API documentation. To view API call definitions and documentation, either navigate to > **APIs** or go to https://crosswork.cisco.com/apiDoc/CiscoCrossworkCloudAPI.

Join the Cisco Community Here to access the Crosswork Developer Hub. You can also access the Cisco Community by navigating to > **Support** > **Community Forum**. Make sure to use and subscribe to the "Crosswork" label to help identify Crosswork Cloud discussions.

Get Started with APIs

You must have Admin privileges to access Crosswork Cloud APIs. The API options will not appear if you do not have Admin privileges. See Change User Permissions, on page 234 for information about changing user permissions.

To view API call definitions and documentation, you *must* be logged into Crosswork Cloud and either click > **APIs** or go to https://crosswork.cisco.com/apiDoc/CiscoCrossworkCloudAPI.

To get started with the APIs, perform the following tasks:

Step 1 To request an API Key, click your user initials in the top-right corner of the Crosswork Cloud Network Insights window, then click **API Key/Tokens**.

Step 2 Click **Add API Key**.

Step 3 Enter a name for the API Key, a description (optional), and a Start and Finish date for the API key, then click **Save**.

Step 4 Click **Create**.

The new API key is created and the Crosswork Cloud application displays the key details. This is the only time that the key is displayed.

Step 5 Click **Copy** to copy the API key so you can save it somewhere secure.

Note Protect your API Key as if it is a password. Because the API Key provides access to your account, make sure you store it securely.

Step 6 See the Crosswork Cloud Network Insights Client Script Example, on page 247 and Crosswork Traffic Analysis Client Script Example, on page 254 sections for examples on how to get started.

API Key Definition

A Crosswork Cloud API Key consists of:

- An API Key, which is a hex encoded, 32-byte symmetric key. Client applications use the API Key to sign REST API requests destined for Crosswork Cloud Network Insights or Crosswork Cloud Traffic Analysis.
- An API Key identifier (ID), which is a unique value for the key and must be included with each signed request. Crosswork Cloud services use the Key ID to retrieve a copy of the API Key to verify the incoming request.

Note Protect your API Key as you would a password. Because the API Key provides access to your account, make sure you store it securely.

A client application uses the API Key to sign all requests that are sent to Crosswork Cloud. Each request includes:

- The request signature
- The API Key ID
- Metadata detailing the fields used to determine the signature

After Crosswork Cloud receives a REST API request, it performs the following steps:

1. Extracts the requested parameters.
2. Uses the API Key ID to retrieve the API Key and associated metadata.
3. Recalculates the signature.
4. Compares the calculated signature with the requested signature.
5. If the calculated and requested signatures match, Crosswork Cloud forwards the request. If the signatures do not match, Crosswork Cloud rejects the request.

Crosswork Cloud Network Insights Client Script

This section contains examples and information on how to use the Crosswork Cloud Network Insights client script.

Client Script Options

The following options are available when running the client script.

```
(ramius) ~> ./crosswork.py -h
usage: crosswork.py [-h] [--uri URI] --key KEY --keyid KEYID
                    [--payload PAYLOAD] [--method {GET,POST}] [--host HOST]
                    [--port PORT]

Exercise the REST API.

optional arguments:
  -h, --help           show this help message and exit
  --uri URI            The URI to run
  --key KEY            A Cisco Crosswork Network Insights API Key
  --keyid KEYID        A Cisco Crosswork Network Insights API Key ID
  --payload PAYLOAD    The name of a file containing JSON data for POST API
                       requests. Note: This option is available only for POST
                       commands.
  --method {GET,POST}  The HTTP method for the request
  --host HOST          The Cisco Crosswork Network Insights URL
  --port PORT          The Cisco Crosswork Network Insights port number
(ramius) ~>
```

Crosswork Cloud Network Insights Client Script Example

The following client script example is written in Python and shows how to create, sign, and execute the Crosswork Cloud Network Insights REST API calls.

```
#!/usr/bin/env python3

#
# Copyright 2019 Cisco Systems Inc.
#
# Licensed under the Apache License, Version 2.0 (the "License");
# you may not use this file except in compliance with the License.
# You may obtain a copy of the License at
#
#     http://www.apache.org/licenses/LICENSE-2.0
#
# Unless required by applicable law or agreed to in writing, software
```

```
# distributed under the License is distributed on an "AS IS" BASIS,
# WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
# See the License for the specific language governing permissions and
# limitations under the License.
#

import argparse
import binascii
import datetime
import hashlib
import hmac
import json
from typing import Dict, Any

import requests
import rfc3339
import sys
import urllib

from string import Template
from urllib.parse import urlparse


class Signature(object):
    # The order and white space usage is very important. Any change
    # can alter the signature and cause the request to fail.
    SIGNATURE_TEMPLATE = Template("""\
$param_method
$param_uri
$param_query_parameters
$param_key_id
$param_timestamp
$param_signature_version
$param_content_sha256
$param_content_type
$param_content_length""")

    def __init__(self, exrest):
        self.exrest = exrest

    def sign(self):
        exrest = self.exrest

        string_to_sign = self.SIGNATURE_TEMPLATE.substitute({
            "param_method": exrest.method.upper(),
            "param_uri": exrest.url_encoded_uri,
            "param_query_parameters": exrest.url_encoded_query_parameters,
            "param_key_id": exrest.key_id,
            "param_timestamp": exrest.timestamp,
            "param_signature_version": exrest.signature_version,
            "param_content_sha256": exrest.content_sha256,
            "param_content_type": exrest.content_type,
            "param_content_length": exrest.content_length
        })

        # Decode the key and create the signature.
        secret_key_data = binascii.unhexlify(exrest.key)
        hasher = hmac.new(secret_key_data, msg=string_to_sign.encode('utf-8'),
digestmod=hashlib.sha256)
        signature = binascii.hexlify(hasher.digest())
        return signature.decode('utf-8')


class ExRest(object):
```

```
    SIGNATURE_VERSION = "1.0"
    CONTENT_TYPE = "application/json"

    HEADER_CONTENT_TYPE = "Content-Type"
    HEADER_CONTENT_LENGTH = "Content-Length"
    HEADER_SIGNATURE_VERSION = "X-Cisco-Crosswork-Cloud-Signature-Version"
    HEADER_TIMESTAMP = "Timestamp"
    HEADER_AUTHORIZATION = "Authorization"

    def __init__(self):
        # Input arguments to the script.
        self.uri = None
        self.payload = None
        self.method = None
        self.host = None
        self.port = None
        self.key = None
        self.key_id = None

        # Values used to calculate the signature.
        self.url_encoded_uri = None
        self.url_encoded_query_parameters = None
        self.timestamp = None
        self.content_sha256 = None
        self.content_length = 0
        self.content_type = self.CONTENT_TYPE
        self.signature_version = self.SIGNATURE_VERSION

    def run(self):
        # Calculate the full URI to be run.
        uri = self.uri[1:] if self.uri.startswith("/") else self.uri
        self.uri = f"https://{self.host}:{self.port}/{uri}"

        # The url encoded uri is used when calculating the request signature.
        parsed_uri = urlparse(self.uri)
        self.url_encoded_uri = urllib.parse.quote(parsed_uri.path, safe="")
        self.url_encoded_query_parameters = urllib.parse.quote(parsed_uri.query)

        # Calculate the rfc3339 timestamp for the request.
        now = datetime.datetime.now()
        self.timestamp = rfc3339.rfc3339(now)

        # Calculate the SHA256 of the body of the request, even if the body is empty.
        self.content_sha256, self.content_length, payload_contents =
self.calculate_content_sha256(self.payload)

        # Calculate a signature for the request.
        signer = Signature(self)
        request_signature_b64 = signer.sign()

        # Create the request object and set the required http headers.
        headers = dict()

        headers[self.HEADER_AUTHORIZATION] = "hmac {}:{}".format(self.key_id,
request_signature_b64)
        headers[self.HEADER_TIMESTAMP] = self.timestamp
        headers[self.HEADER_CONTENT_TYPE] = self.content_type
        headers[self.HEADER_SIGNATURE_VERSION] = self.SIGNATURE_VERSION

        session = requests.Session()

        response = session.request(self.method, self.uri, data=payload_contents,
headers=headers)
```

```
            parsed_response: Dict[str, Any] = dict()
            if len(response.content) > 0:
                content = response.content.decode('utf-8')
                try:
                    parsed_response = json.loads(content)
                except ValueError:
                    parsed_response = dict()
                    parsed_response["Message"] = content.strip()

            if response.status_code != 200:
                parsed_response["HttpStatus"] = response.status_code

            print(json.dumps(parsed_response, indent=2))

        def calculate_content_sha256(self, payload):
            if payload:
                try:
                    with open(payload) as fd:
                        payload_contents = fd.read()
                except Exception as error:
                    raise Exception(f'Cannot read payload file {payload}: {error}')
            else:
                payload_contents = ""

            hasher = hashlib.sha256()
            hasher.update(payload_contents.encode('utf-8'))

            content_sha256 = binascii.hexlify(hasher.digest())

            return content_sha256.decode('utf-8'), len(payload_contents), payload_contents


    def main():
        parser = argparse.ArgumentParser(description="Exercise the REST API.")

        parser.add_argument("--uri", default="/api/beta/truefalse/1/200",
                            help="The URI to run")

        parser.add_argument("--key", required=True,
                            help="A Cisco Crosswork Network Insights API Key")

        parser.add_argument("--keyid", required=True,
                            help="A Cisco Crosswork Network Insights API Key ID")

        parser.add_argument("--payload",
                           help="The name of a file containing JSON data for POST API requests")


        parser.add_argument("--method", choices=["GET", "POST"], default="GET",
                            help="The HTTP method for the request")

        parser.add_argument("--host", default="crosswork.cisco.com",
                            help="The Cisco Crosswork Network Insights URL")

        parser.add_argument("--port", type=int, default=443,
                            help="The Cisco Crosswork Network Insights port number")

        # Parse the arguments
        args = parser.parse_args()

        exrest = ExRest()

        exrest.uri = args.uri
        exrest.payload = args.payload
```

```
        exrest.method = args.method
        exrest.host = args.host
        exrest.port = args.port
        exrest.key = args.key
        exrest.key_id = args.keyid

        exrest.run()


if __name__ == "__main__":
        sys.exit(main())
```

How to Use the Client Script

This example walks you through the following tasks:

- Making a simple call from the client script.
- Adding prefixes with a POST command using the `payload` option and a configuration file.

Before you begin

Before running the script, request the API key (see Get Started with APIs, on page 245). For more information on APIs, click  from the Crosswork Cloud UI and click the **APIs** link.

Step 1 Run the script:

```
crosswork.py --uri '/api/beta/sourcedata?prefix=64.54.195.0%2F24&max=5' --key '<yourKeyHere>' --keyid
 '<yourKeyIdHere>'
```

Example result:


```
{
  "data": [
    {
      "prefix": "64.54.195.0/24",
      "action": "ADD",
      "peerRemoteAsn": 22024,
      "timestamp": "2021-10-20T18:32:03Z",
      "origin": "IGP",
      "originAs": 5653,
      "asPath": [
        {
          "asn": [
            22024
          ]
        },
        {
          "asn": [
            6461
          ]
        },
        {
          "asn": [
            5653
          ]
        }
      ],
      "unicastPrefixType": "ADJ_RIB_IN",
      "nextHop": "4.4.94.118/32",
```

```
      "peerRemoteId": "549",
      "roaGenTime": "2021-06-29T05:25:53.844840001Z"
    },
    {
      "prefix": "64.54.195.0/24",
      "action": "ADD",
      "peerRemoteAsn": 202365,
      "timestamp": "2022-01-21T10:25:58Z",
      "origin": "IGP",
      "originAs": 5653,
      "med": {},
      "communities": [
        3792306480,
        3792306677,
        57866,
        41441,
        41441
      ],
      "asPath": [
        {
          "asn": [
            202365
          ]
        },
        {
          "asn": [
            57866
          ]
        },
        {
          "asn": [
            6461
          ]
        },
        {
          "asn": [
            5653
          ]
        }
      ],
      "unicastPrefixType": "ADJ_RIB_IN",
      "nextHop": "5.255.90.109/32",
      "peerRemoteId": "248",
      "roaGenTime": "2021-10-05T10:07:45.504885118Z"
    },
(truncated)
```


Step 2 Add prefixes with a POST command and a configuration file:

```
crosswork.py --uri '/api/beta/provision' --key '<yourKeyHere>' --keyid '<yourKeyIdHere>' --payload
"config.json" --method "POST"
```

Example of config.json file contents:

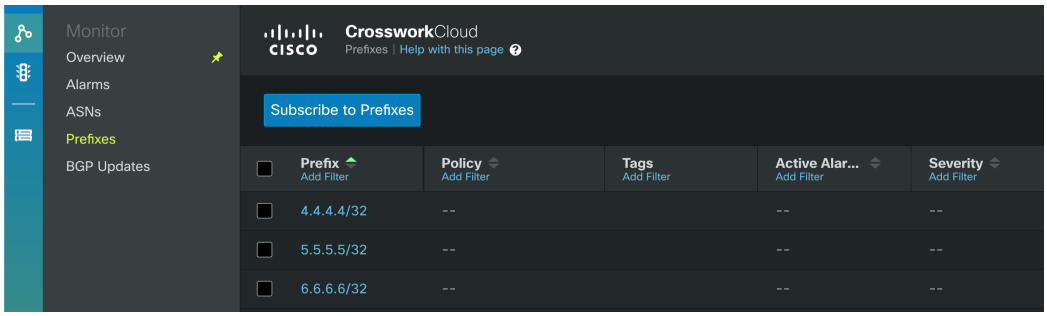
```
{
  "operations": [
    {
      "setPrefixRequest": {
        "prefix": "4.4.4.4/32"
      },
      "o_creat": true,
      "o_excl": true
    },
    {
      "setPrefixRequest": {
```

```
        "prefix": "5.5.5.5/32"
      },
      "o_creat": true,
      "o_excl": true
    },
    {
      "setPrefixRequest": {
        "prefix": "6.6.6.6/32"
      },
      "o_creat": true,
      "o_excl": true
    },
    {
      "setPrefixRequest": {
        "prefix": "2001:30:102::/48"
      },
      "o_creat": true,
      "o_excl": true
    }
  ]
}
```

Results example:

```
{
  "results": [
    {
      "setPrefixResponse": {
        "prefix": "4.4.4.4/32"
      }
    },
    {
      "setPrefixResponse": {
        "prefix": "5.5.5.5/32"
      }
    },
    {
      "setPrefixResponse": {
        "prefix": "6.6.6.6/32"
      }
    },
    {
      "setPrefixResponse": {
        "prefix": "2001:30:102::/48"
      }
    }
  ]
}
```

UI Results example:



Crosswork Traffic Analysis Client Script Example

The following script examples are written in Python. You will need **python/get_traffic_example.py** and **python/cctraffic/cctraffic.py** to execute the Crosswork Traffic Analysis APIs. Prior to running `get_traffic_example.py`, you must do the following:

1. Install python dependencies: `pip3 install -r requirements.txt`
2. Set the API bearer token: `export TOKEN=<token string>`
3. Edit the get_traffic_example.py file. Replace the following with the correct values: `api_version`, `device_name`, `start` and `end`.

After editing the `get_traffic_example.py` file, run the script: `python3 get_traffic_example.py`

Script Example: get_traffic_example.py

```
# get_traffic_example.py

import os
import sys
from cctraffic import CCTrafficRestClient

host = "https://crosswork.cisco.com"
api_version = "beta"
device_name = "flow-automation-1"

# start and end may be supplied as:
#   - ISO 8601 datetime string
#   - unix timestamp in seconds since 1970
#   - now
#   - "<number> <unit> ago" where unit can be: "seconds", "minutes", "hours", "days".
start = "7 days ago"
end = "now"

if "TOKEN" in os.environ:
    token = os.environ["TOKEN"]
else:
    print("Bearer token not found. Set bearer token with: export TOKEN=<token string>")
    sys.exit(-1)

client = CCTrafficRestClient(host, token, version=api_version, debug=False)

print(f"GetDevice for {device_name}")
device_info = client.GetDevice(device_name)
```

```
device_id = device_info["deviceId"]
print(f"Found device ID for {device_name}: {device_id}")

print(f"Traffic by interface for {device_name}")
traffic_for_my_device = client.GetInterfaceCounterTrafficTotals(start, end, device_id)
interface_name = traffic_for_my_device[0]["interfaces"][0]["interfaceName"]

print(f"Traffic by ASN for {device_name}/{interface_name}")
asn_traffic_for_my_device_interface = client.GetNetFlowTrafficTotalsByDevice(start, end,
device_id, interface=interface_name, asn_breakdown=True)

print(f"Traffic by Prefix for {device_name}/{interface_name}")
prefix_traffic_for_my_device_interface = client.GetNetFlowTrafficTotalsByDevice(start, end,
 device_id, interface=interface_name, prefix_breakdown=True)

asn = asn_traffic_for_my_device_interface[0]["interfaces"][0]["asns"][0]["asn"]
device_prefix =
prefix_traffic_for_my_device_interface[0]["interfaces"][0]["prefixes"][0]["prefix"]

print(f"Traffic by Prefix for {device_name}/{interface_name} ASN {asn}")
prefix_traffic_for_my_device_interface_asn = client.GetNetFlowTrafficTotalsByDevice(
    start, end, device_id, interface=interface_name, asn=asn, asn_breakdown=True)

print(f"Traffic by Prefix")
prefix_traffic = client.GetNetFlowTrafficTotalsByPrefix(start, end)
prefix = prefix_traffic[0]["prefix"]

print(f"Traffic by Device for {prefix}")
device_traffic_for_prefix = client.GetNetFlowTrafficTotalsByPrefix(start, end, prefix)

print(f"Time series for {device_name}")
time_series_for_device = client.GetInterfaceCounterTrafficTimeSeries(start, end, device_id)

print(f"Time series for {device_name}/{interface_name}")
time_series_for_interface = client.GetInterfaceCounterTrafficTimeSeries(start, end, device_id,
 interface=interface_name)

print(f"Time series for {device_name}/{interface_name} {device_prefix}")
time_series_for_prefix = client.GetNetFlowTrafficTimeSeriesByDevice(start, end, device_id,
 interface=interface_name, prefix=device_prefix)

print(f"Time series for {device_name}/{interface_name} {asn}")
time_series_for_asn = client.GetNetFlowTrafficTimeSeriesByDevice(start, end, device_id,
interface=interface_name, asn=asn)
```

Script Example: cctraffic.py

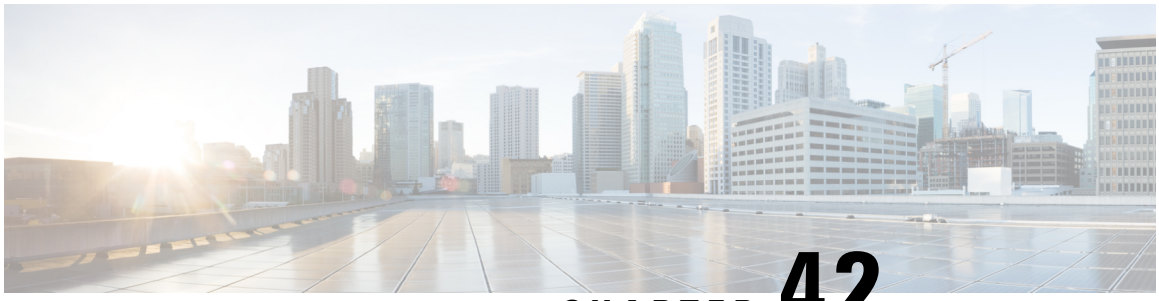
```
# cctraffic.py
# Contains a very simple REST client to demonstrate how to call the Crosswork Cloud Traffic
 APIs
# Copyright (c) 2021 Cisco Systems, Inc. and others.  All rights reserved.

import requests
from .util import UrlEncode

import urllib3
urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)


class CCTrafficRestClient:

    def __init__(self, host: str, token, version: str = "v1", debug: bool = False):
        self.version = version
        self.host = host
        self.debug = debug
```

```
        self.headers = {"content-type": "application/json", "Authorization": f"Bearer
{token}"}

    def DoApiCall(self, url):
        if self.debug == True:
            print(url)
        response = requests.get(url, headers=self.headers, verify=False)
        if self.debug == True:
            print(response.status_code)
            print(response.content)
        return response

    def GetDevice(self, device_name: str):
        url = f"{self.host}/api/{self.version}/devices?name={device_name}"
        response = self.DoApiCall(url)
        if response.status_code != 200:
            return ""
        return response.json()["devices"][0]["deviceInfo"]

    def GetInterfaceCounterTrafficTotals(self, start: str, end: str, device_id: str = ""):
        start = UrlEncode(start)
        end = UrlEncode(end)

        if device_id == "":
            url = f"{self.host}/api/{self.version}/devices/statistics/totals"
        else:
            url =
f"{self.host}/api/{self.version}/devices/{device_id}/interfaces/statistics/totals"

        url += f"?format=totals&timeStart={start}&timeEnd={end}"
        response = self.DoApiCall(url)
        if response.status_code != 200:
            return ""
        return response.json()["devices"]

   def GetNetFlowTrafficTotalsByDevice(self, start: str, end: str, device_id: str, interface:
 str,
                                       asn: int = 0, prefix: str = "", asn_breakdown: bool
 = False, prefix_breakdown: bool = False):
        interface = UrlEncode(UrlEncode(interface))
        prefix = UrlEncode(UrlEncode(prefix))
        start = UrlEncode(start)
        end = UrlEncode(end)

        if asn != 0:
            url =
f"{self.host}/api/{self.version}/traffic/devices/{device_id}/interfaces/{interface}/asns/{asn}/prefixes"

        elif asn_breakdown:
            url =
f"{self.host}/api/{self.version}/traffic/devices/{device_id}/interfaces/{interface}/asns"
        elif prefix_breakdown:
            url =
f"{self.host}/api/{self.version}/traffic/devices/{device_id}/interfaces/{interface}/prefixes"


        url += f"?format=totals&timeStart={start}&timeEnd={end}"
        response = self.DoApiCall(url)
        if response.status_code != 200:
            return ""
        return response.json()["devices"]

    def GetNetFlowTrafficTotalsByPrefix(self, start: str, end: str, prefix: str = "",
device_id: str = ""):
```

```
        prefix = UrlEncode(UrlEncode(prefix))
        start = UrlEncode(start)
        end = UrlEncode(end)

        if prefix == "":
            url = f"{self.host}/api/{self.version}/traffic/prefixes"
        elif device_id == "":
            url = f"{self.host}/api/{self.version}/traffic/prefixes/{prefix}/devices"
        else:
            url =
f"{self.host}/api/{self.version}/traffic/prefixes/{prefix}/devices/{device_id}/interfaces"

        url += f"?format=totals&timeStart={start}&timeEnd={end}"
        response = requests.get(url, headers=self.headers, verify=False)
        if response.status_code != 200:
            return ""
        return response.json()["prefixes"]

    def GetInterfaceCounterTrafficTimeSeries(self, start: str, end: str, device_id: str,
interface: str = ""):
        interface = UrlEncode(UrlEncode(interface))
        start = UrlEncode(start)
        end = UrlEncode(end)

        if interface == "":
            url = f"{self.host}/api/{self.version}/devices/{device_id}/statistics/totals"
        else:
            url =
f"{self.host}/api/{self.version}/devices/{device_id}/interfaces/{interface}/statistics/totals"


        url += f"?format=timeseries&timeStart={start}&timeEnd={end}"
        response = requests.get(url, headers=self.headers, verify=False)
        if response.status_code != 200:
            return ""
        return response.json()["devices"]

    def GetNetFlowTrafficTimeSeriesByDevice(self, start: str, end: str, device_id: str,
interface: str, asn: int = 0, prefix: str = ""):
        interface = UrlEncode(UrlEncode(interface))
        prefix = UrlEncode(UrlEncode(prefix))
        start = UrlEncode(start)
        end = UrlEncode(end)

        if asn == 0 and prefix != "":
            url =
f"{self.host}/api/{self.version}/traffic/devices/{device_id}/interfaces/{interface}/prefixes/{prefix}"

        elif asn != 0 and prefix == "":
            url =
f"{self.host}/api/{self.version}/traffic/devices/{device_id}/interfaces/{interface}/asns/{asn}"

        else:
            url =
f"{self.host}/api/{self.version}/traffic/devices/{device_id}/interfaces/{interface}/asns/{asn}/prefixes/{prefix}"


        url += f"?format=timeseries&timeStart={start}&timeEnd={end}"
        response = self.DoApiCall(url)
        if response.status_code != 200:
            return ""
        return response.json()["devices"]
```

PART IX

Purchase and Manage Subscriptions



CHAPTER 42

View Subscription Plan Options

View Subscription Plan Options

To view available subscription plans and what features are included, click here or navigate to > **Purchase** > **Tier Information** tab. Within each product tab you can expand categories and compare the various features that are available in each tier.

If you would like to purchase a subscription, see Purchase through a Cisco Partner or Reseller or Purchase through Amazon Web Services (AWS) Marketplace.

For more information about each Crosswork Cloud product, see one of the following data sheets:

- Crosswork External Route Analysis (Network Insights)
- Crosswork Traffic Analysis
- Crosswork Trust Insights

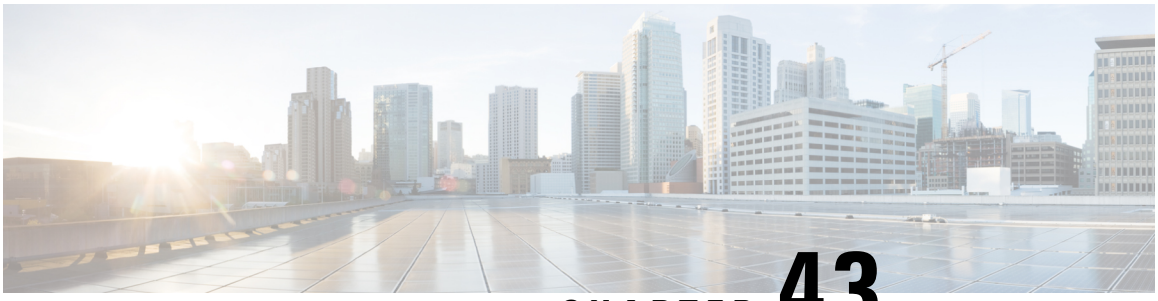
Free Subscription Plan Requirement

To maintain a free subscription plan, at least *one* of the following requirements must be met:

- A user in an organization must log into Crosswork Cloud within the last 90 days.
- An organization must maintain an active peer (with a complete internet routing table) in Crosswork Cloud Network Insights.
- An organization must have an active entitlement for a different module.

To avoid automatic termination, please purchase a minimum of one IP route prefix to monitor with Crosswork Cloud Network Insights through a Cisco Partner or Reseller, or purchase through Amazon Web Services (AWS) Marketplace.

For information on what features are available with a free subscription plan click here or navigate to > **Purchase** > **Subscription Tiers** tab within Crosswork Cloud.

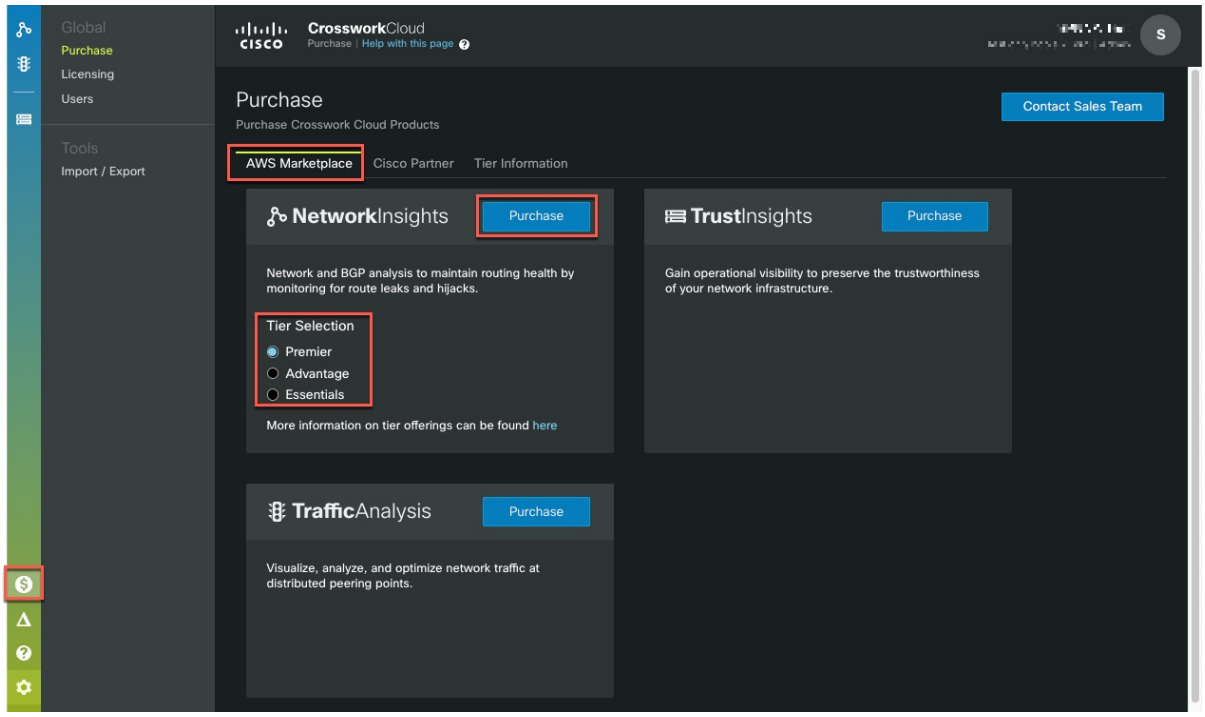


CHAPTER 43

Purchase Crosswork Cloud

You can purchase Cisco Crosswork Cloud subscriptions using one of the following methods:

Purchase through Amazon Web Services (AWS) Marketplace



Note Click any of the images to view them in full-size.

Before you begin

The simplest way to purchase Crosswork Cloud is through AWS Marketplace within Crosswork Cloud itself. To purchase Crosswork Cloud directly from AWS Marketplace, click Purchase Directly from AWS Marketplace.

Please have the following accounts set up:

- Cisco Connection Online (CCO)
- Crosswork Cloud
- AWS Marketplace—You ***must*** have a valid AWS payment method set up and current or you will run into errors.

Note This procedure assumes you already have these accounts set up and are logged into Crosswork Cloud.

Step 1 In the main window, click  in the bottom-left corner.

Step 2 Click the **AWS Marketplace** tab.

Step 3 If purchasing Crosswork Cloud Network Insights, select the appropriate licensing tier (Premier, Advantage, or Essentials) and click **Purchase**. Otherwise, click **Purchase** for either Crosswork Cloud Trust Insights or Crosswork Cloud Traffic Analysis.

You will be taken to the AWS Marketplace website.

Step 4 Log into AWS Marketplace. The Crosswork Cloud product purchase page appears.

Step 5 Click **View purchase options** and enter all required fields.

Step 6 Click **Create contact** and review the information.

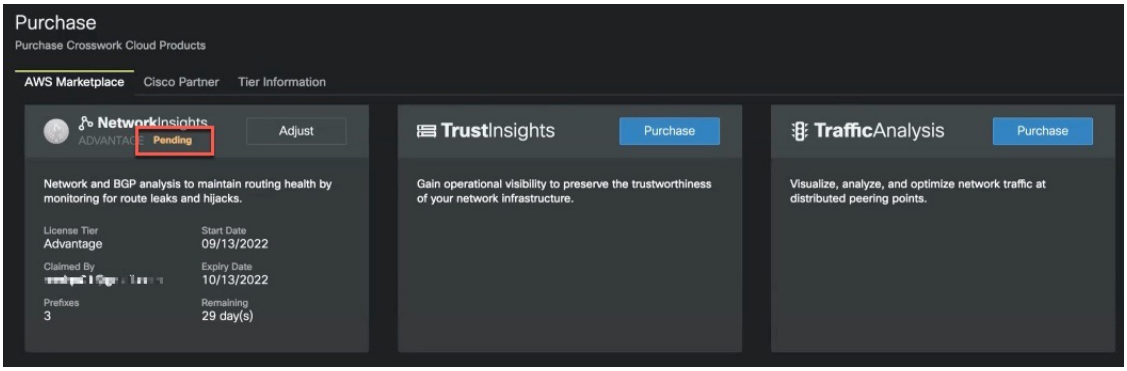
Step 7 Click **Pay now**. A Congratulations message appears.

Step 8 Click **Set up your account** to be taken to the **Purchasing** page within Crosswork Cloud.

Example:

Step 9 The Crosswork Cloud product may have a **Pending** status for a couple minutes until all AWS Marketplace data details have been received.

Example:



Step 10 Confirm your subscription by navigating to > **Licensing** > **Entitlement** tab > <***Crosswork-Cloud-Product***>. You should see the product and subscription details listed in the table.

Step 11 After you have successfully purchased a Crosswork Cloud subscription, you will receive an email with a subscription ID. Keep a copy of the email and store the ID in case you need it to activate your Crosswork Cloud entitlement at a later time. For more information, see Activate a Subscription or Trial, on page 237.

Purchase Directly from AWS Marketplace

To purchase Crosswork Cloud directly from AWS Marketplace, do the following:

Before you begin

You ***must*** have an AWS Marketplace account and confirm that a payment method has been configured.

The following procedure provides steps on how to purchase Crosswork Cloud directly from AWS Marketplace. If you are purchasing Crosswork Cloud for your organization or on behalf of someone else, please have the administrator's (end user) email address on hand. If you will be a Crosswork Cloud adminstrator, please have the following accounts set up to streamline the purchasing process:

- Cisco Connection Online (CCO)
- Crosswork Cloud

Note If you have not registered for CCO or Crosswork Cloud accounts, you will be directed to each website's registration screen during the purchasing process.

Step 1 Log into AWS Marketplace and set up a payment method if one hasn't been set up for your account.

Step 2 In the **Search** field enter **Crosswork Cloud** and select the product you want to purchase.

Step 3 Click **View purchase options** and enter all required fields.

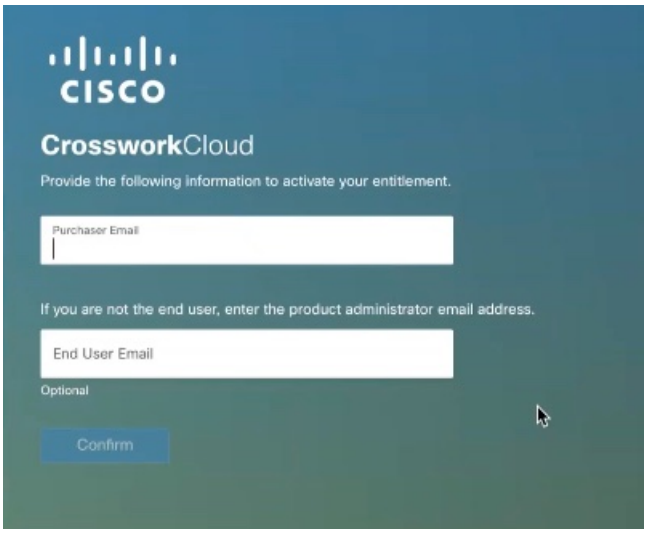
Step 4 Click **Create contact**and review the information.

Step 5 Click **Pay now**. A Congratulations message appears.

Step 6 Click **Set up your account** and you will be directed to the **Purchasing** page in Crosswork Cloud.

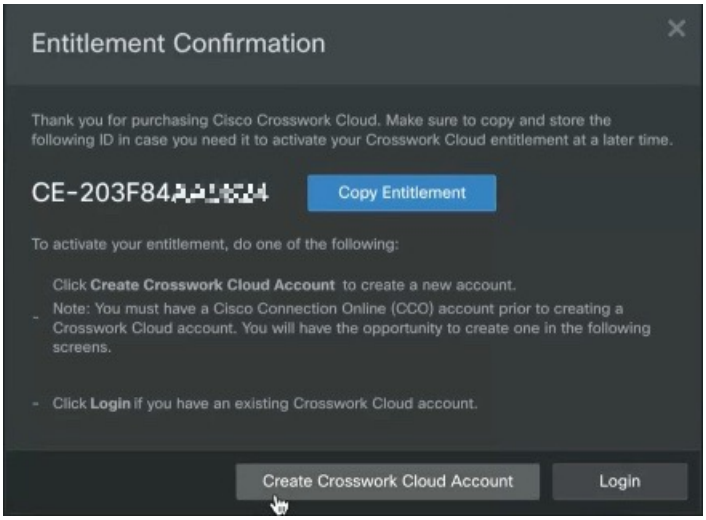
Step 7 If you are not currently logged into Crosswork Cloud, enter your email and, if you are not going to be the end user, the product administrator’s email address in the following window and click **Confirm**.

Example:



Step 8 An email will be sent to both the email addresses containing some information and the entitlement ID. The Crosswork Cloud administrator should keep a copy of the email and store the entitlement ID in case you need it to activate your Crosswork Cloud entitlement at a later time. For more information, see Activate a Subscription or Trial, on page 237.

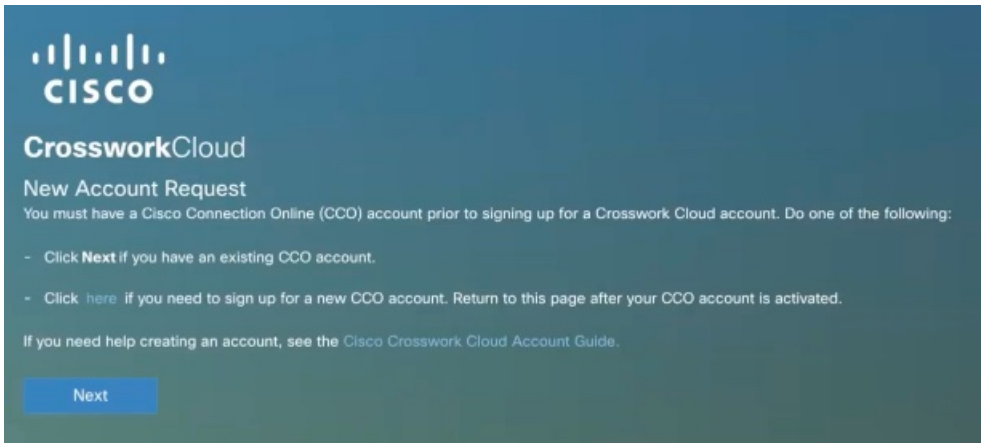
Figure 10: Entitlement Confirmation Example



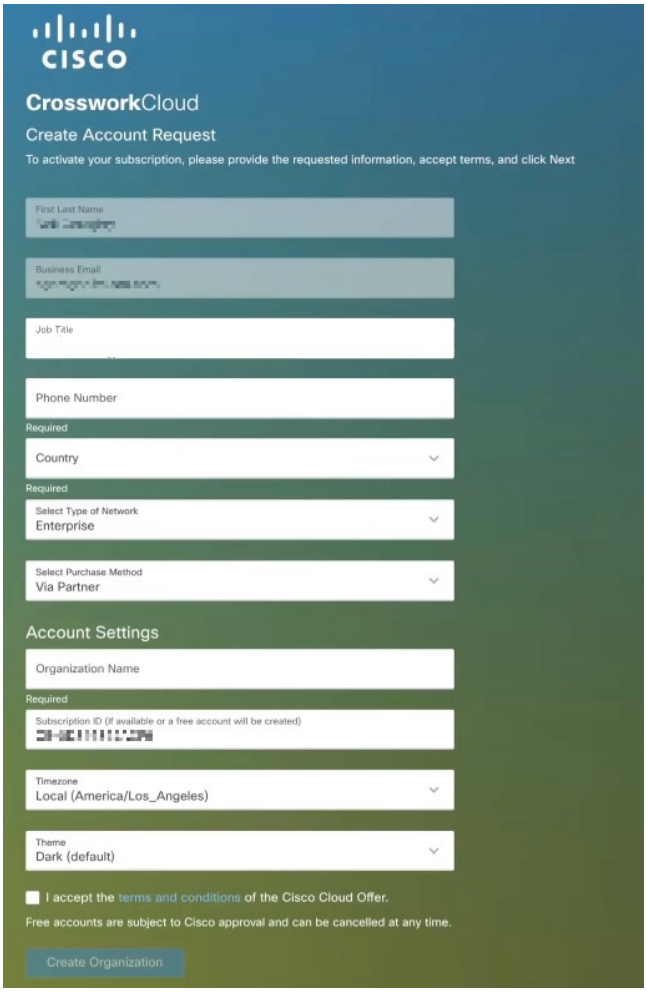
From this point on, unless the Purchaser would like to create a Crosswork Cloud account, the Crosswork Cloud administrator should perform the next steps.

Step 9 If you do *not* have a Crosswork Cloud account, click **Create Crosswork Cloud Account** and follow the prompts to create an account and configure an organization. If you do have a Crosswork Cloud account, go to **Step 10**.

Example:



Note After you have created a CCO account (or if you have an existing CCO account), you will be prompted to fill out some information to create a Crosswork Cloud account.

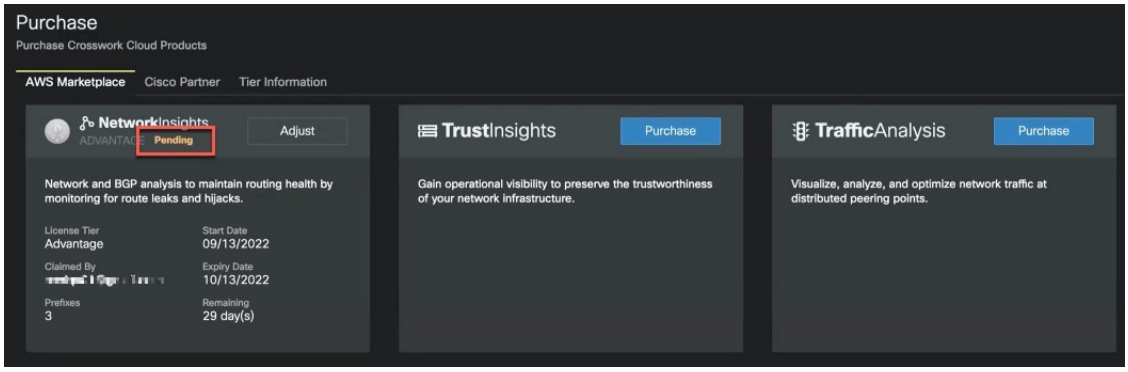


Step 10 If you have a Crosswork Cloud account, click **Login**.

Step 11 Enter your credentials and click **Login**. A Success message appears stating that your subscription has been claimed.

Step 12 Click **OK** to close the message. The **Crosswork Cloud Purchase** page appears. The entitlement is automatically associated with the tenancy organization you have previously configured. The Crosswork Cloud product may have a **Pending** status until all AWS Marketplace data details have been received.

Example:



Step 13 Confirm your subscription by navigating to > **Licensing** > **Entitlement** tab > <***Crosswork-Cloud-Product***>. You should see the product and subscription details listed in the table.

Purchase through a Cisco Partner or Reseller

To purchase Crosswork Cloud through a Cisco Partner or Reseller:

Step 1 In the main window, click in the bottom-left corner.

Step 2 Click the **Sales Purchase** tab.

Step 3 Click **Contact Sales Team**.

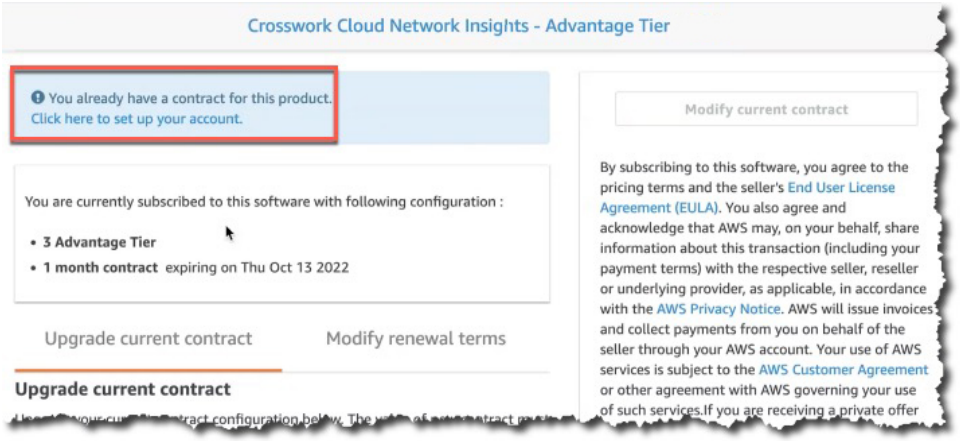
Step 4 Select the Crosswork Cloud product you are interested in purchasing and click **Send**.

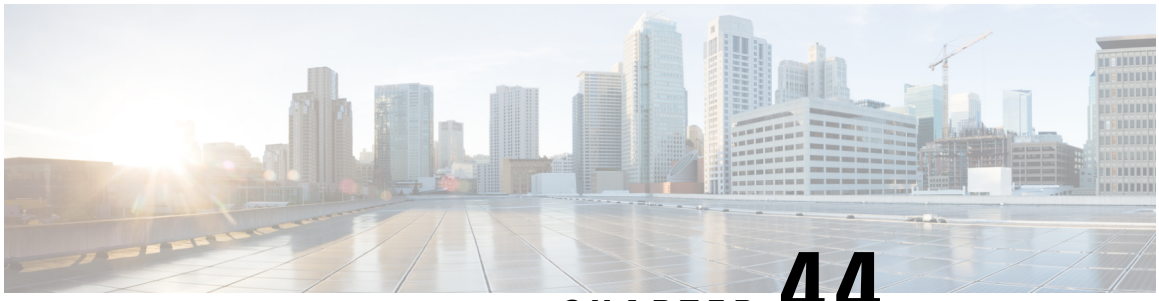
Troubleshoot Purchasing Issues

This topic provides you with some helpful hints and items you can check for when you come across AWS Marketplace purchasing problems. If you still have purchasing issues, click > **Purchasing Support** > **Payment Support**, enter a description of the issue you are having, and click **Submit**.

- Confirm that a payment method has been set up in AWS Marketplace. For more information on valid payments that AWS Marketplace accepts, go to https://aws.amazon.com/premiumsupport/knowledge-center/accepted-payment-methods/.
- If in Crosswork Cloud, the product still remains in the **Pending** status, refresh the page and click > **Licensing** > **Entitlement** tab > <***Crosswork-Cloud-product***> to confirm if the product is listed. Sometimes it takes a few minutes until Crosswork Cloud retrieves AWS subscription information.

- In AWS Marketplace, go to the Crosswork Cloud product purchase page again and select **Click here to set up your account** to resume the purchasing process.





CHAPTER 44

Activate a Subscription or Trial

Activate a Subscription or Trial

You can activate a subscription in Crosswork Cloud.

Note You must have admin privileges to activate a subscription. See User Roles, on page 234 for more information.

Before you begin

To activate a subscription, you must have one or more subscription IDs which are given or emailed to you after purchasing Crosswork Cloud.

Step 1 In the main window, click in the bottom-left corner.

Step 2 Click **Licensing**.

Step 3 To activate a subscription:

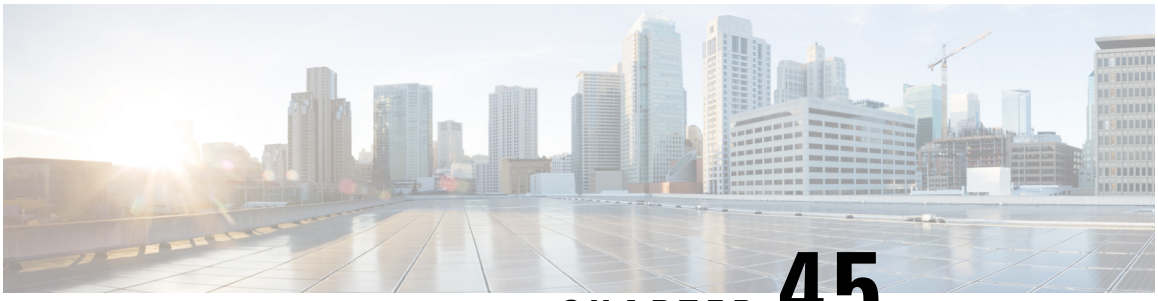
a) Click **Entitlement > External Route Analysis**, **Trust Insights**, or **Traffic Analysis** tab.

b) Click **Claim Subscription** and enter your subscription IDs in the text box. To add multiple subscription IDs, separate each ID with a comma or enter each ID on a new line.

Step 4 To request a Crosswork Cloud product trial version:

a) Click the **Trials** tab.

b) Click **Request** next to the Crosswork Cloud product you would like to try. Accept the terms and click **Start Trial**.



CHAPTER 45

View Your Subscription and Licenses

View Subscription and Trial Details

To view details about subscriptions, current licenses, and active trials you have, do the following:

Step 1 In the main window, click  in the bottom-left corner.

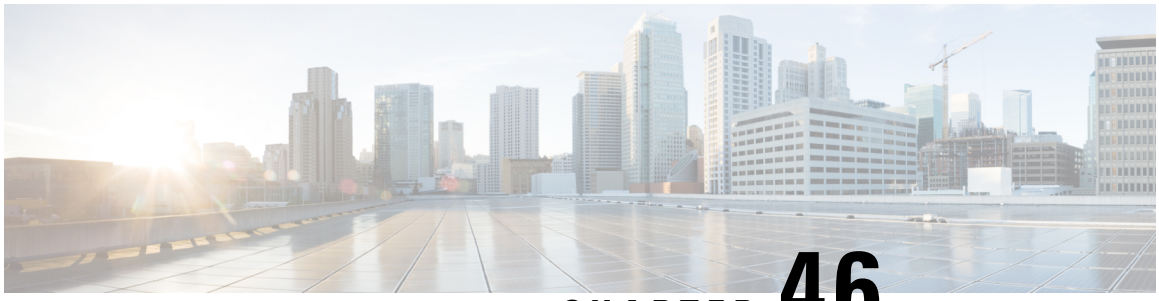
Step 2 Click **Licensing**.

Step 3 To view subscription and licensing details, click the **Entitlement** tab and select the Crosswork Cloud product you are interested in.

Step 4 To view the number of trials that are active and available, click the **Trials** tab.

What to do next

To cancel or update your subscription, see Modify a Subscription, on page 275.



CHAPTER 46

Modify a Subscription

Update a Subscription

To increase the number of permitted prefixes (for Crosswork External Route Analysis), or cancel a Crosswork Cloud subscription, do the following:

Note To change a subscription that was purchased in AWS Marketplace to a different tier, you must first cancel the old subscription, and purchase the new one.

Step 1 In the main window, click $ in the bottom-left corner.

Step 2 If your subscription was purchased through AWS:

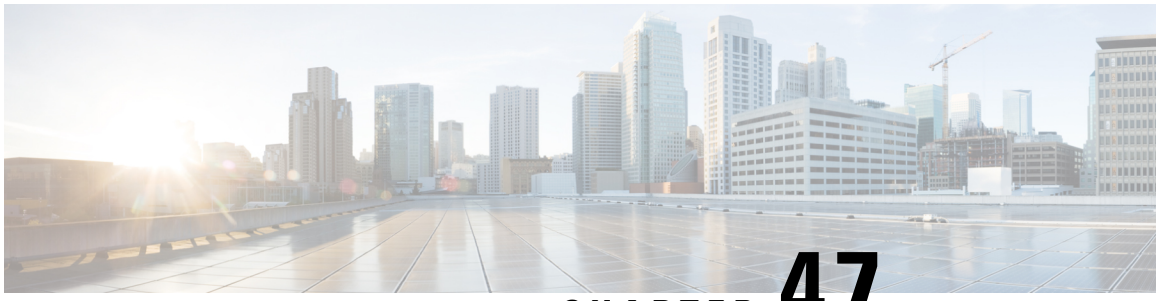
a) Click the **AWS Purchase** tab.

b) Click **Adjust** for the product you are modifying a subscription for. You are taken to the AWS Marketplace website.

c) Click **View purchase options** and make the necessary changes.

d) Click **Modify current contract**. After you have successfully modified a Crosswork Cloud subscription, you will receive a confirmation email.

Step 3 If your subscription was purchased through a Cisco Partner or Reseller, click **Contact Sales Team** in the top-right corner to get in contact with a Crosswork Cloud representative who can help you modify your subscription.



CHAPTER 47

Transfer a Subscription to Another Organization

Transfer a Subscription to Another Organization

To move your subscription to another organization, you must first remove the subscription ID from the previous organization and then assign it to the new organization.

Step 1 Make sure you have the entitlement ID on hand prior to transferring it to another organization. The entitlement ID was initially emailed to the Crosswork Cloud administrator when the Crosswork Cloud account was set up.

Step 2 Log into the organization that is currently associated with the subscription and go to > **Licensing**.

Step 3 Click **Entitlement** tab > <***Crosswork-Cloud-product***>.

Step 4 Check the checkbox next to the subscription you want to transfer.

Step 5 Click the **Remove** link that appears.

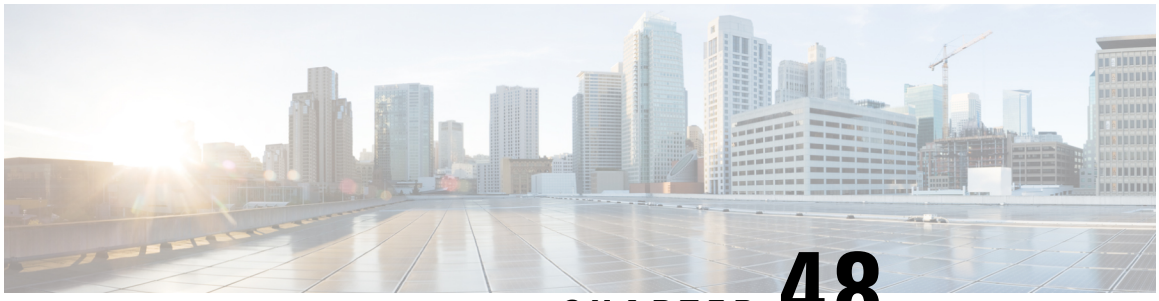
Step 6 Click **Remove** in the confirmation window to confirm subscription removal.

Step 7 Navigate to the organization that you want to subscribe to and go to > **Licensing**.

Step 8 Click **Entitlement** tab > <***Crosswork-Cloud-product***>.

Step 9 Click **Claim Subscription** (located in the top right of the page).

Step 10 Enter the entitlement ID, and click **Claim**.



CHAPTER 48

Modify Organization Name

Modify Organization Name

You can modify the name of your organization.

Step 1 In the main window, click in the bottom-left corner.

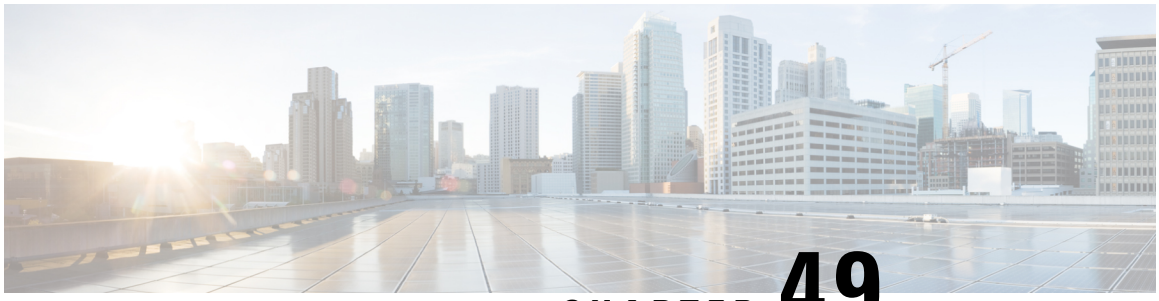
Step 2 Click **Licensing**.

Step 3 Click **Edit**.

Step 4 Enter a new organization name, then click **Save**.

PART X

Modify User Settings



CHAPTER 49

Modify User Settings

Change User Interface Theme

You can choose one of three user interface themes:

- Dark (default)
- Light
- High-contrast

Change the theme by following these steps:

Step 1 Click your user initials in the top-right corner, then select **My Settings**.

Step 2 From the **Theme** drop-down list, select a theme, then click **Save**.

Modify Time Zone

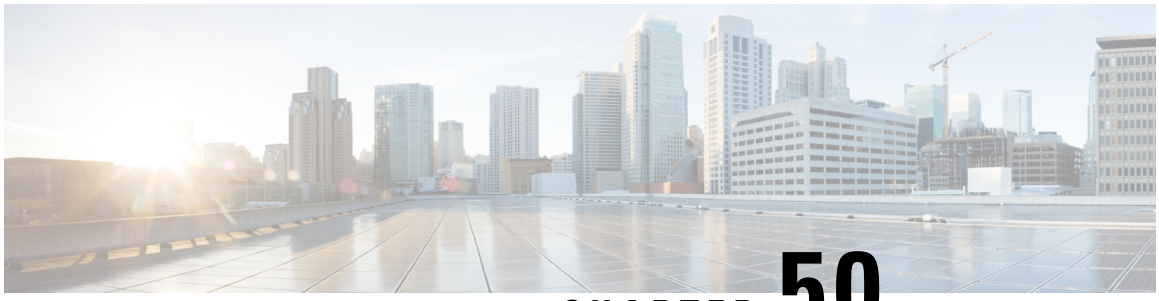
You can modify the time zone for the system.

Step 1 Click your user initials in the top-right corner, then select **My Settings**.

Step 2 From the **Timezone** drop-down list, select a time zone, then click **Save**.

PART XI

Alarm Descriptions



CHAPTER 50

Alarm Descriptions

Alarm Descriptions

This section contains a list of alarms and linked descriptions. Alarms are triggered when a rule is violated in a policy.

Table 34: Crosswork Cloud Network Insights Alarms

Unexpected AS Prefix, on page 289	Prefix Withdrawal, on page 301	Upstream AS Change, on page 313
AS Origin Violation, on page 291	ROA Expiry, on page 303	Valid AS Path Violation, on page 315
New AS Path Edge, on page 293	ROA Failure, on page 305	Peer Down, on page 317
AS Path Length Violation, on page 295	ROA Not Found, on page 307	Advertised Prefix Count, on page 319
Parent Aggregate Change, on page 297	DNS Root Prefix Withdrawal, on page 309	Prohibited IP Prefix, on page 321
Prefix Advertisement, on page 299	Subprefix Advertisement, on page 311	

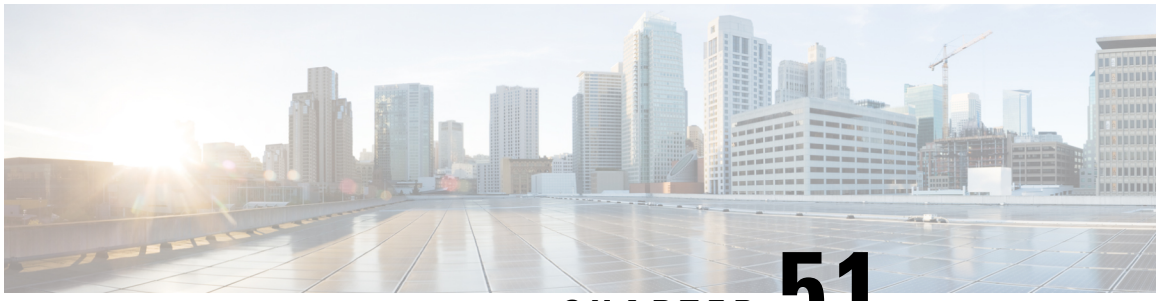
Table 35: Crosswork Cloud Traffic Analysis Alarms

Gateway Connectivity, on page 323	Device Connectivity, on page 325	Interface TX Utilization, on page 327
Interface RX Utilization, on page 329	Prefix Utilization, on page 331	

Table 36: Crosswork Cloud Trust Insights Alarms

Gateway Connectivity, on page 323	Device Running Configuration Change, on page 337	Hardware Integrity Validation

Device Connectivity, on page 325	Device SSH Host Key Violation	Mismatched Files
Device Certificate Expiring, on page 333	Dossier Collection Failure, on page 341	Package Validation
Device Certificate Violation	Expired Device Certificate, on page 343	Unknown Files



CHAPTER 51

Unexpected AS Prefix

Unexpected AS Prefix

This alarm detects unexpected changes for an AS where a new prefix was not previously there. Any prefix that originates from a monitored BGP AS is a violating prefix if it is not subscribed to by your organization (subject to peer thresholds).

Possible Problem Detected

This alarm can help identify an unexpected change or route leak scenario for an AS where a new prefix was not previously observed.

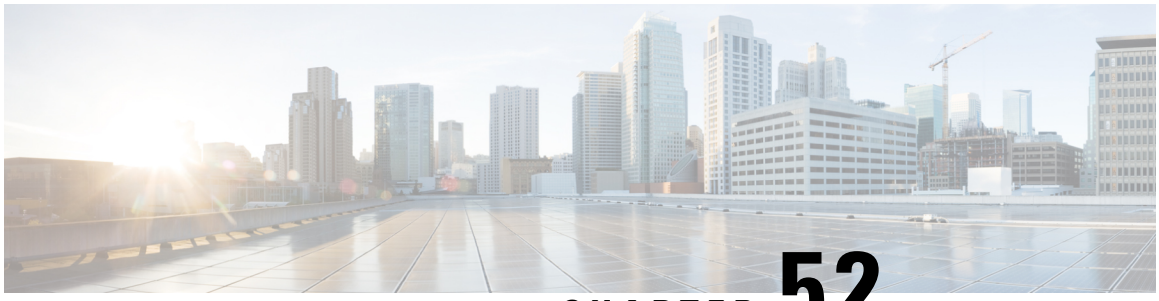
Relevant Alarm Rule Configurations

The following options must be configured when adding this alarm rule to an ASN policy configuration (**External Routing Analysis > Configure > Policies > Add Policy > ASN Policy > Add Rule > Unexpected AS Prefix**):

- Alarm Thresholds (per advertised prefix)
- Configure Prefixes

Example

You create an ASN Policy with the **Unexpected AS Prefix** alarm rule and linked to a monitored AS 15169. You are also subscribed to all prefixes that are expected to originate from AS 15169. Due to a misconfiguration, prefix 8.8.0.0/24 is leaked from the AS. At the same time, prefix 9.9.0.0/24 is advertised correctly, but is not subscribed to. Subject to peer thresholds, both these events cause the alarm to trigger. You can then correct the configuration to withdraw prefix 8.8.0.0/24 and subscribe to prefix 9.9.0.0/24 which clears the alarm.



CHAPTER 52

AS Origin Violation

AS Origin Violation

This alarm detects when any advertisement for the monitored prefix with origin AS is not in the **AS Origin List** list. This is a violating advertisement and could represent a prefix hijack attempt, especially if the AS path length in the advertisement is shorter than legitimate advertisements.

Note It is useful to know which of your peers may be doing something wrong (leaking route information or having some type of misconfiguration) so that you can address the problem right away. A **My Peers** rule is available for this alarm with certain Crosswork Cloud subscriptions. The **My Peers** option follows BGP updates *only* from your Add Peers, whereas **All Peers** follow BGP updates from your peers *and* global peers. To configure this option, see Add Crosswork Cloud Network Insights Policies, on page 77.

Possible Problem Detected

This alarm can help identify route leaks or a prefix hijack.

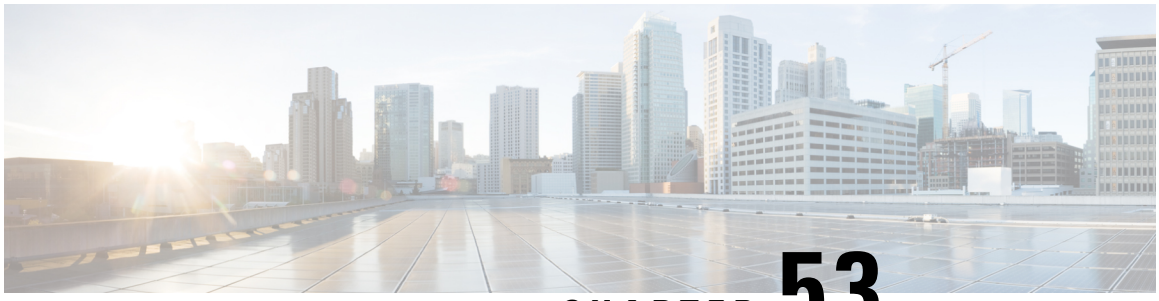
Relevant Alarm Rule Configurations

The following options should be configured when adding this alarm rule to a Prefix policy configuration (**External Routing Analysis > Configure > Policies > Add Policy > Prefix Policy > Add Rule > AS Origin Violation**):

- Alarm Thresholds
- Allowed Origin ASNs

Example

You create a Prefix Policy with the **AS Origin Violation** alarm rule with for prefix 8.8.8.0/24 and it is configured with an AS Origin List field value of 15169. However, an observed BGP update is received with 8.8.8.0/24 and an origin AS of 109. This alarm triggers because AS 109 is not included in the AS Origin List.



CHAPTER 53

New AS Path Edge

New AS Path Edge

This alarm detects a new AS peering that was not previously observed before.

Man-in-the-Middle (MITM) attacks involve an attacker injecting their own AS into the AS path of a prefix, thereby directing traffic for the prefix through their AS. To avoid detection of the attack, MITM attacks are usually short-lived and target a small set of prefixes.

Another source of a transient AS peering could be an operator error which is corrected quickly.

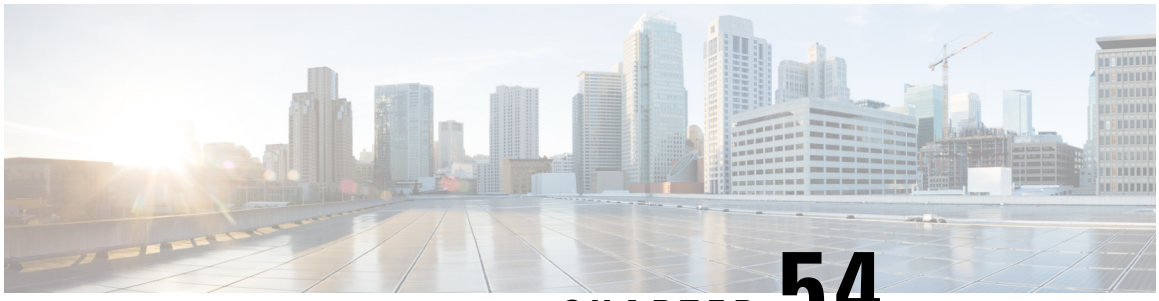
Note An AS peering relationship that appears in the AS path of a large number of prefixes advertised by many peers or is long-lived, is most likely a legitimate network configuration change and Crosswork Cloud Network Insights does not alert on those.

Possible Problem Detected

This alarm helps identify potential MITM attacks or an operator error.

Example

You create a Prefix policy with the **New AS Path Edge** alarm rule and is linked to prefix 8.8.0.0/24. The alarm triggers when Crosswork Cloud Network Insights detects that prefix 8.8.0.0/24 is advertised with an AS path that includes suspicious AS peerings (peerings that have not been previously seen across all paths for all prefixes or are new). After a certain amount of time, Crosswork Cloud Network Insights determines that these AS peering relationships are long-lived. After it determines that the peering relationships are long-lived and legitimate, the alarm is cleared.



CHAPTER 54

AS Path Length Violation

AS Path Length Violation

Detects when an AS path length for a configured prefix exceeds an upper or lower threshold. This alarm detects when an observed AS path falls below a lower threshold or exceeds an upper threshold for the AS Path Length.

The BGP AS path impacts the latency of prefixes, but is also an important tie-breaking step in BGP bestpath selection (the highest non-configurable attribute used in *bestpath* selection). Since shorter AS paths are preferred, this property can be exploited by a hijacker. You must configure an expected range for the AS path length for the monitored prefix. An advertised AS path length outside this range is a violating advertisement

Note It is useful to know which of your peers may be doing something wrong (leaking route information or having some type of misconfiguration) so that you can address the problem right away. A **My Peers** rule is available for this alarm with certain Crosswork Cloud subscriptions. The **My Peers** option follows BGP updates *only* from your Add Peers, whereas **All Peers** follow BGP updates from your peers *and* global peers. To configure this option, see Add Crosswork Cloud Network Insights Policies, on page 77.

Possible Problem Detected

This alarm can help identify route leaks or hijacks. It can also help monitor latency of monitored prefixes.

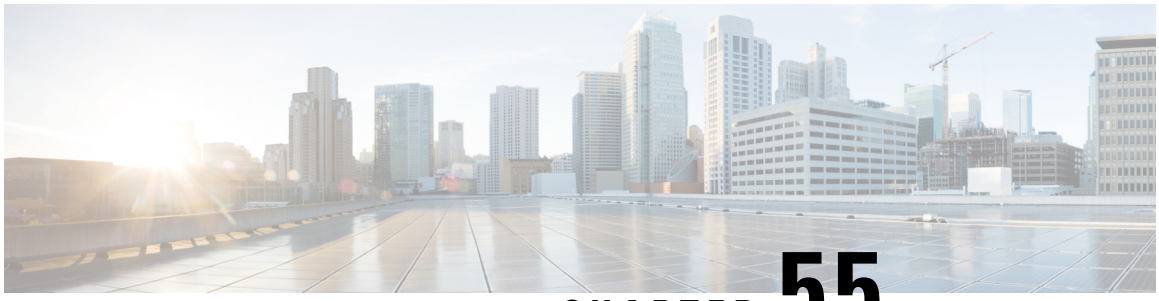
Relevant Alarm Rule Configurations

The following options must be configured when adding this alarm rule to a Prefix policy configuration (**External Routing Analysis > Configure > Policies > Add Policy > Prefix Policy > Add Rule > AS Path Length Violation**):

- Alarm Thresholds
- Allowed AS path length range

Example

You create a Prefix policy with the **AS Path Length Violation** alarm rule and linked to prefixes 8.8.0.0/24 and 9.9.0.0/24. Prefix 8.8.0.0/24 is leaked by the user via a different peering point resulting in a shorter AS path which triggers the alarm. The alarm clears when prefix 8.8.0.0/24 is advertised via legitimate advertisements (a path length within the allowed range). Later, peering relationships change in the upstream path from prefix origin 9.9.0.0/24 (legitimately or due to a MITM attack) causing it to be advertised with a longer AS path. You might have little control of these upstream relationships and need to change the configured AS path range for the alarm to clear.



CHAPTER 55

Parent Aggregate Change

Parent Aggregate Change

This alarm detects an unexpected supernet or threshold violation.

A network operator is usually aware of their immediate supernet prefix (aggregate or summary) of their advertised prefixes, other aggregated higher order supernets, and their origin AS. The user must configure at least one set of expected IPv4 and IPv4 supernets by specifying their Classless inter-domain routing (CIDR) prefix-lengths. The user can also enforce that the observed aggregates originate from a list of allowed Origin ASs.

Note It is useful to know which of your peers may be doing something wrong (leaking route information or having some type of misconfiguration) so that you can address the problem right away. A **My Peers** rule is available for this alarm with certain Crosswork Cloud subscriptions. The **My Peers** option follows BGP updates *only* from your Add Peers, whereas **All Peers** follow BGP updates from your peers *and* global peers. To configure this option, see Add Crosswork Cloud Network Insights Policies, on page 77.

Possible Problem Detected

This alarm can help identify the accidental withdrawal or route-leak of summary prefixes.

Relevant Alarm Rule Configurations

The following options must be configured when adding this alarm rule to a Prefix policy configuration (**External Routing Analysis > Configure > Policies > Add Policy > Prefix Policy > Add Rule > Parent Aggregate Change**):

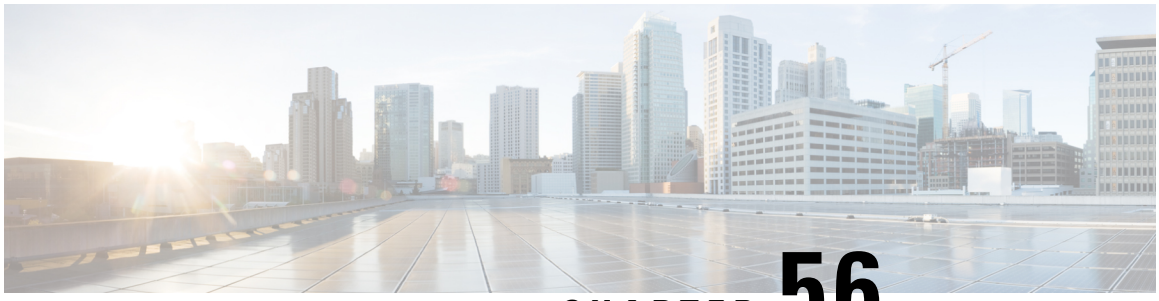
- Alarm Thresholds (per advertised aggregate)
- Allowed Origin ASNs (optional)
- Allowed IPv4/IPv6 supernets

Example

You create a Prefix policy with the **Parent Aggregate Change** alarm rule and is linked to prefix 8.8.0.0/24. The policy is configured with allowed IPv4 aggregate prefix lengths [22, 9] and an Allowed Origin AS 3356. The following events will trigger an alarm:

- An expected supernet of 8.8.0.0/22 is hijacked (prefix originates from an unexpected origin AS).
- An aggregate, prefix 8.8.0.0/20, is advertised and is identified as a potential leak.

The alarms are cleared when either the leak or hijack is resolved, or the user changes the alarm configuration to indicate that these aggregate advertisements are legitimate.



CHAPTER 56

Prefix Advertisement

Prefix Advertisement

This alarm rule detects when a prefix is advertised and reports if it exceeds the threshold trigger.

Note It is useful to know which of your peers may be doing something wrong (leaking route information or having some type of misconfiguration) so that you can address the problem right away. A **My Peers** rule is available for this alarm with certain Crosswork Cloud subscriptions. The **My Peers** option follows BGP updates *only* from your Add Peers, whereas **All Peers** follow BGP updates from your peers *and* global peers. To configure this option, see Add Crosswork Cloud Network Insights Policies, on page 77.

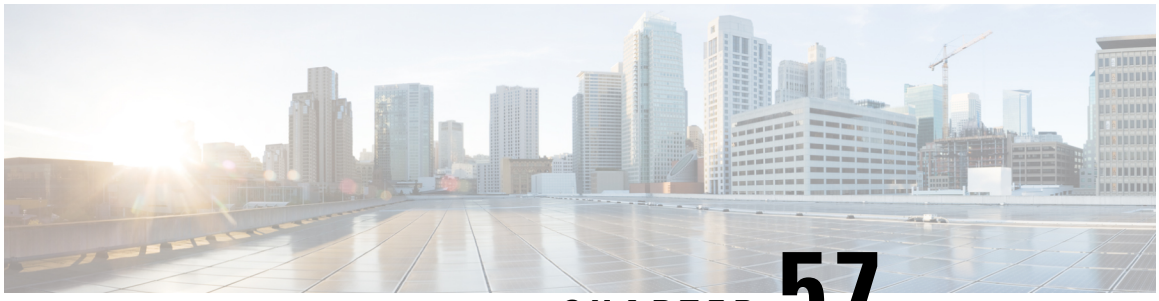
Possible Problem Detected

This alarm helps identify a route leak or unexpected change for a configured prefix.

Relevant Alarm Rule Configurations

The following options must be configured when adding this alarm rule to a Prefix policy configuration (**External Routing Analysis > Configure > Policies > Add Policy > Prefix Policy > Add Rule > Prefix Advertisement**):

- Alarm Thresholds



CHAPTER 57

Prefix Withdrawal

Prefix Withdrawal

This alarm detects when a peer withdraws a prefix.

The withdrawal of a prefix from a few BGP peers does not necessarily mean that the prefix is unreachable since there are multiple paths to reach a prefix. However, if a large enough number of peers withdraw off the prefix in a geographical area, the reachability of the prefix can be degraded. It is recommended that thresholds for this alarm are set higher than other alarms to suppress noise caused by router flap.

Note It is useful to know which of your peers may be doing something wrong (leaking route information or having some type of misconfiguration) so that you can address the problem right away. A **My Peers** rule is available for this alarm with certain Crosswork Cloud subscriptions. The **My Peers** option follows BGP updates *only* from your Add Peers, whereas **All Peers** follow BGP updates from your peers *and* global peers. To configure this option, see Add Crosswork Cloud Network Insights Policies, on page 77.

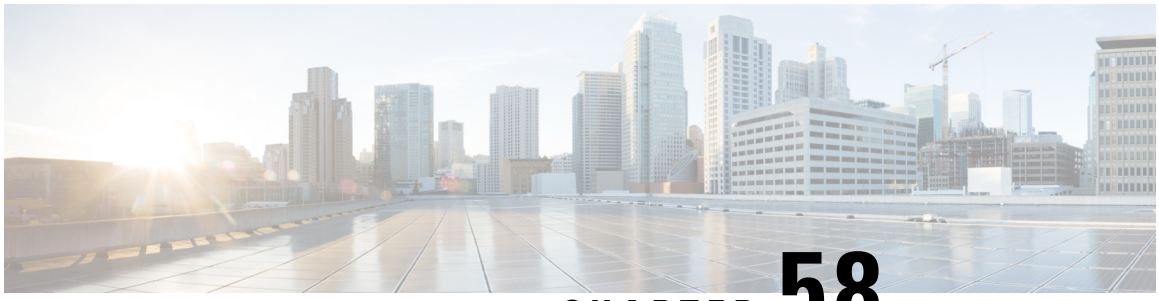
Possible Problem Detected

This alarm can help identify a misconfiguration resulting in prefix withdrawal.

Relevant Alarm Rule Configurations

The following options must be configured when adding this alarm rule to a Prefix policy configuration (**External Routing Analysis > Configure > Policies > Add Policy > Prefix Policy > Add Rule > Prefix Withdrawal**):

- Alarm Thresholds



CHAPTER 58

ROA Expiry

ROA Expiry

This alarm alerts you before the expiration date of a Route Origin Authorization (ROA) record. An ROA record is created by an operator claiming ownership of the resource (advertised prefix) and distributed cryptographically by Regional Internets Registries (RIRs) or other services such as the Routing Assets Database (RADb). For more information, see ripe.net.

You can specify then number of days to be alerted in advance of the ROA record expiring. This is an informational alarm. You can take actions to create a new record to avoid possible filtering of their prefixes by routers. This alarm activates if the prefix is covered by any ROA records and the prefix will not have a valid ROA record at any given time between now and the configured trigger interval (now + **Days to Trigger Before Expiration**). In particular, the alarm does not activate if there is a mix of expired and unexpired records, as long as every point in time in the configured interval has some unexpired covering record.

Possible Problem Detected

This alarm detects a pending lack of ROA coverage.

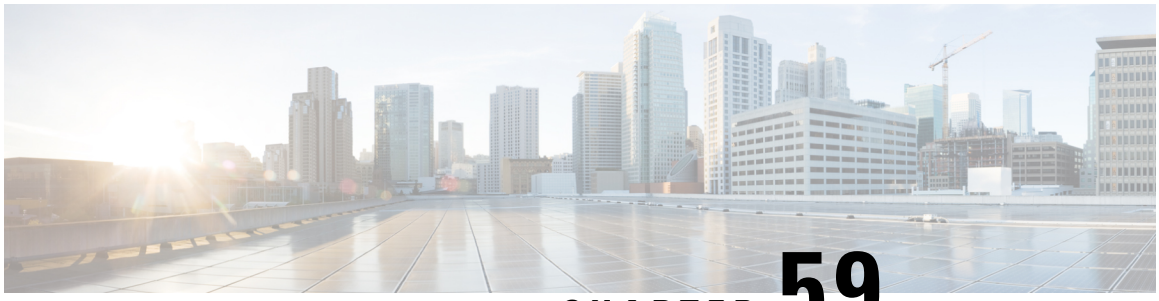
Relevant Alarm Rule Configurations

The following option must be configured when adding this alarm rule to a Prefix policy configuration (**External Routing Analysis > Configure > Policies > Add Policy > Prefix Policy > Add Rule > ROA Expiry**):

- Days to trigger before the expiration of an ROA record.

Example

You create a Prefix policy with the **ROA Expiry** alarm rule and linked to prefix 8.8.0.0/24 with 30 **Days to Trigger Before Expiration**. The alarm triggers if prefix 8.8.0.0/24 is covered by multiple ROA records and Crosswork Cloud Network Insights detects that all of these records have already expired or will expire in less than 30 days. To clear the alarm, you should create at least one ROA record for 8.8.0.0/24 covering the trigger time interval.



CHAPTER 59

ROA Failure

ROA Failure

This alarm indicates whether the ROA validity state of the monitored prefix is invalid. see Any advertisement for the monitored prefix with origin AS that is not in any ROA record covering the prefix is a violating advertisement. The alarm clears either due to the addition of ROA records that include all observed Origin ASNs of the prefix or all records expiring. Specifically, this alarm does not activate if there are no ROA records (none existed or all are expired).

For more information on ROAs, see ripe.net.

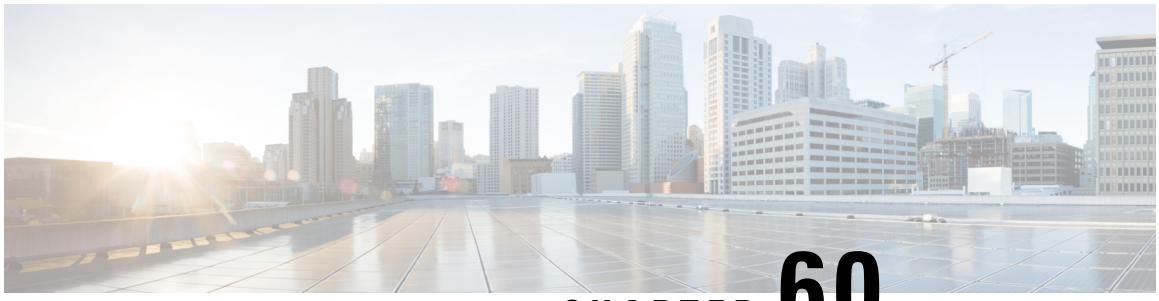
Possible Problem Detected

This alarm can help identify prefix hijack attempts.

Relevant Alarm Rule Configurations

The following option must be configured when adding this alarm rule to a Prefix policy configuration (**External Routing Analysis > Configure > Policies > Add Policy > Prefix Policy > Add Rule > ROA Failure**):

- Alarm Thresholds



CHAPTER 60

ROA Not Found

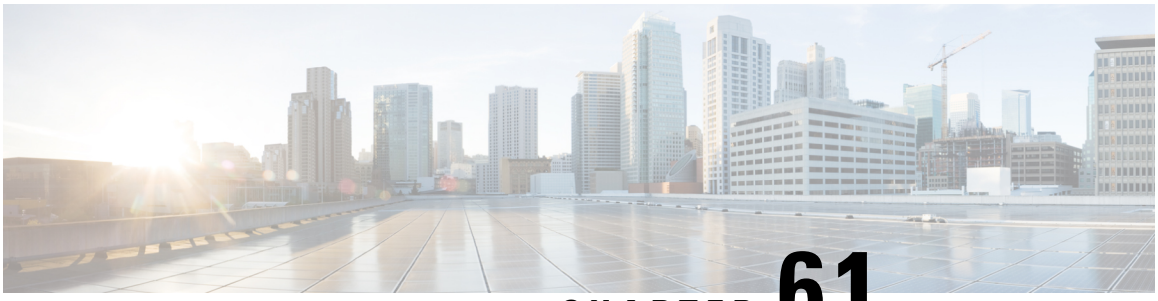
ROA Not Found

A prefix can have multiple ROA records covering it. This alarm triggers if the monitored prefix has no ROA records (none existed or they have expired). This can avoid the prefix from being dropped by routers that implement RTR protocol.

For more information on ROAs, see ripe.net.

Possible Problem Detected

This is an informational alarm alerting the user that a monitored prefix has no ROA records.



CHAPTER 61

DNS Root Prefix Withdrawal

DNS Root Prefix Withdrawal

Public DNS Root servers, which includes those assigned by IANA and provided by OpenDNS and Google, are necessary for normal router operation to participate in public internet routing. This alarm monitors a set of prefixes (netblocks) to which the DNS server address belongs. It alerts the user if any prefix in the set is withdrawn.

Note This alarm differs from the Prefix Withdrawal alarm because these prefixes do not add to the total amount of prefixes consumed by the user in their subscription, and the withdrawal is from a peer linked to the alarm rule.

Possible Problem Detected

This alarm detects if the well known DNS Root Server prefix is withdrawn from a monitored peer's routing table. This alarm can help identify a misconfiguration of the internet router resulting in withdrawal of DNS Root Servers.

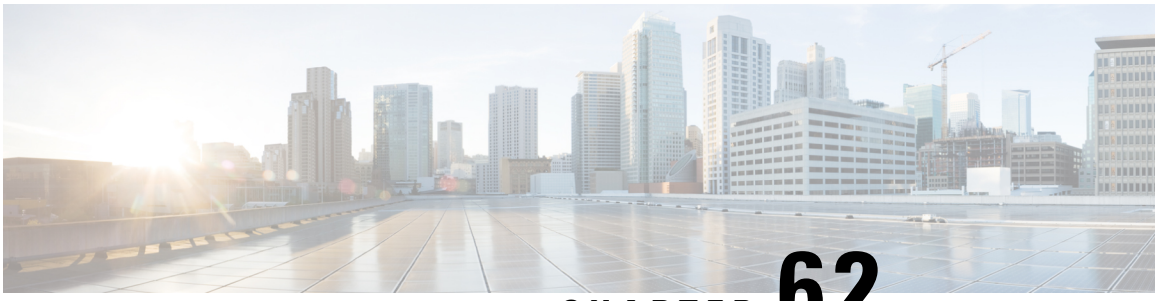
Relevant Alarm Rule Configurations

The following options must be configured when adding this alarm rule to a Peer policy configuration (**External Routing Analysis > Configure > Policies > Add Policy > Peer Policy > Add Rule > DNS Root Prefix Withdrawal**):

- Monitored DNS Root Servers

Example

You create a Peer Policy with the **DNS Root Prefix Withdrawal** alarm rule and is linked to peer RTR1. You select to be alerted for prefixes 198.41.0.0/24 (A root server) and 2001:7fd::/48 (K root server). The alarm activates if either of these prefixes is withdrawn by RTR1 and clears when both are advertised.



CHAPTER 62

Subprefix Advertisement

Subprefix Advertisement

A hijacker can redirect traffic for a portion of the IP space covered by the monitored prefix by installing a new subprefix (since a router will prefer the more specific route over a less specific one). The hijacker can also install a new route for an existing subprefix. To detect these hijack attempts, you can configure a list of allowed Origin ASNs of the subprefixes. For this alarm, the violating advertisement is when either the advertised *subprefix* and its peer threshold is in violation.

Possible Problem Detected

This alarm can help identify route leaks or the hijacking of a subprefix of the monitored prefix.

Relevant Alarm Rule Configurations

The following options should be configured when adding this alarm rule to a Prefix policy configuration (**External Routing Analysis > Configure > Policies > Add Policy > Prefix Policy > Add Rule > Subprefix Advertisement**):

- Configure Prefixes
- Alarm Thresholds per advertised subprefix (Peers to Resolve and Peers to Trigger)
- Allowed Origin ASNs

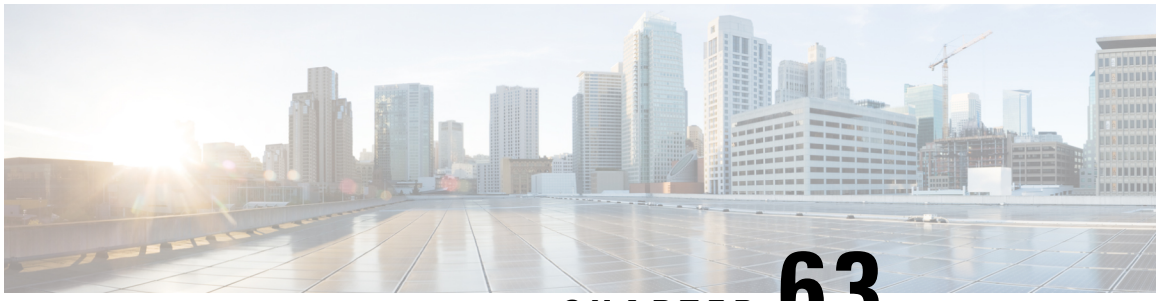
Note Toggle the **Use Origin ASNs** option to **No** to ignore the Origin ASNs list. An alarm will trigger for all ASNs if the Origin ASNs list is ignored.

- Max IPv4/IPv6 Length—Option to ignore subprefix masks longer than the configured **IPv4/IPv6 Max Length** is available. The maximum IPv4 length must be greater than 8 and the maximum IPv6 length must be greater than 16.

Example

You create a Prefix policy with the **Subprefix Advertisement** alarm rule and is linked to prefix 8.8.0.0/24. The following subprefix advertisements occur and triggers an alarm:

- An unexpected subprefix 8.8.0.5/30 is advertised. In this case, you had allocated this prefix to a new administrative organization and it is being advertised for the first time from a new origin AS. To clear this alarm, configure Crosswork Cloud Network Insights to subscribe to the *subprefix* 8.8.0.5/30, or its new origin AS should be added to the list of allowed Origin ASNs.
- An unexpected subprefix 8.8.0.4/30 is advertised. This may indicate either a route leak or a hijack. In order to clear this alarm, 8.8.04/30 should be withdrawn.



CHAPTER 63

Upstream AS Change

Upstream AS Change

A BGP operator has control over their peering relationships through outbound policies (for example, which upstream ASs can propagate a prefix). This alarm detects a route leak to an existing peer, who should not propagate the prefix. The user must configure a list of allowed Upstream ASNs. Any advertisement for the monitored prefix with 1-hop left ASN in the upstream AS path that is not in the list, is a violating advertisement.

Note It is useful to know which of your peers may be doing something wrong (leaking route information or having some type of misconfiguration) so that you can address the problem right away. A **My Peers** rule is available for this alarm with certain Crosswork Cloud subscriptions. The **My Peers** option follows BGP updates *only* from your Add Peers, whereas **All Peers** follow BGP updates from your peers *and* global peers. To configure this option, see Add Crosswork Cloud Network Insights Policies, on page 77.

Possible Problem Detected

This alarm can help identify route leaks of a monitored prefix.

Relevant Alarm Rule Configurations

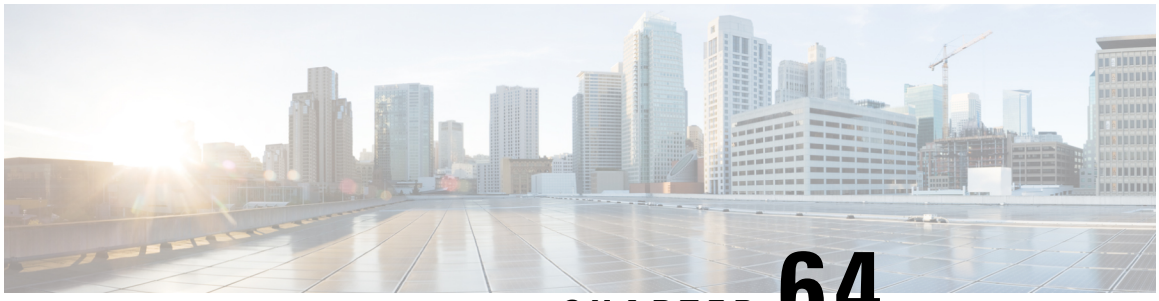
The following options must be configured when adding this alarm rule to a Prefix policy configuration (**External Routing Analysis > Configure > Policies > Add Policy > Prefix Policy > Add Rule > Upstream AS Change**):

- Alarm Thresholds
- Allowed Upstream ASNs

Example

You create a Prefix policy with the **Upstream AS Change** alarm rule with allowed Upstream ASNs [293,1221] and linked to prefixes 8.8.0.0/24. Prefix 8.8.0.0/24 is advertised by a peer or peers with AS path [2711, 1299, 3356]. Subject to thresholding, the alarm triggers because AS1299 is not an allowed upstream ASN. The

alarm clears when the route with the offending AS path is withdrawn or you add AS1229 to the list of allowed upstream ASNs.



CHAPTER 64

Valid AS Path Violation

Valid AS Path Violation

This alarm detects when a prefix advertisement AS path does not match a specified ASN pattern.

Crosswork Network Insights compares the configured **Valid AS Path Pattern** with the advertised AS path of a prefix. The ASN pattern is the expected sequence of AS numbers in order, separated by spaces, and ends with the origin AS such as 107 3462 109. You can use operators to express complex patterns. If the patterns do not match, Crosswork Network Insights triggers the alarm to be active.

Note It is useful to know which of your peers may be doing something wrong (leaking route information or having some type of misconfiguration) so that you can address the problem right away. A **My Peers** rule is available for this alarm with certain Crosswork Cloud subscriptions. The **My Peers** option follows BGP updates *only* from your Add Peers, whereas **All Peers** follow BGP updates from your peers *and* global peers. To configure this option, see Add Crosswork Cloud Network Insights Policies, on page 77.

Example pattern: [0-]* 806 * 200

- Valid AS path: 1900 1731 806 100 200
- Violating AS path: 1900 1731 807 100 200
- Violating AS path: 1900 1731 806 150 100 200

Possible Problem Detected

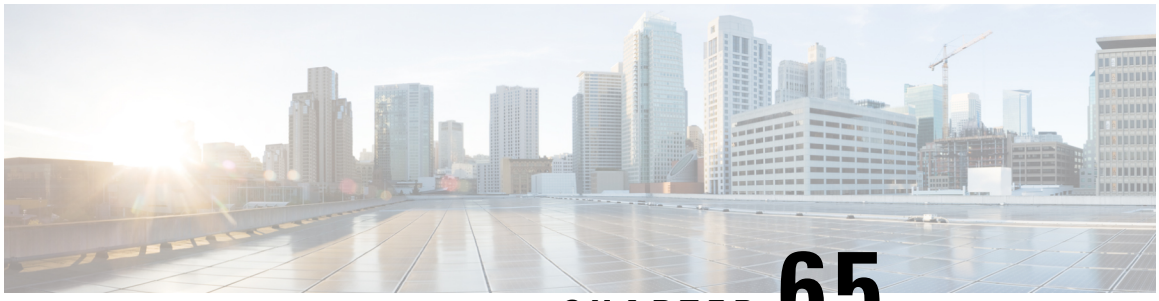
This alarm detects unexpected BGP AS-path changes indicating potential MITM attacks or latency degradation.

Relevant Alarm Rule Configurations

The following options must be configured when adding this alarm rule to a Prefix policy configuration (**External Routing Analysis > Configure > Policies > Add Policy > Prefix Policy > Add Rule > Valid AS Path Violation**):

- Valid AS path pattern (Click **Edit**)

- Alarm Thresholds



CHAPTER 65

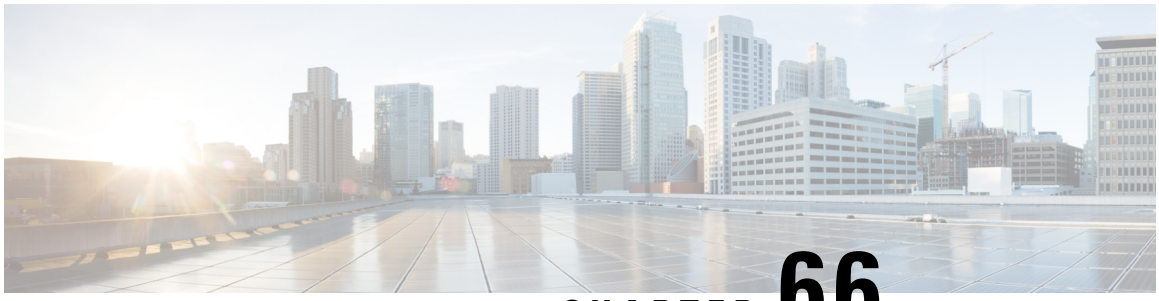
Peer Down

Peer Down

This alarm monitors the health of the peering session between Crosswork Cloud Network Insights and a monitored peer. It is a possible problem if the peering session between Crosswork Cloud Network Insights and a monitored peer is not in an *established* state when it is expected to be. The alarm clears when the peering session is in an established state.

Possible Problem Detected

This alarm can help identify a problem with the BGP process on the monitored peer, or a hardware or software issue that may affect the peering.



CHAPTER 66

Advertised Prefix Count

Advertised Prefix Count

This alarm monitors the size of the RIB of a monitored peer. Crosswork Cloud Network Insights collects statistics that relate to all monitored peers (including the number of prefixes advertised by each peer to Crosswork Cloud Network Insights) at regular intervals. You must configure at least one IPv4/IPv6 address family range for the number of prefixes expected to be advertised to Crosswork Cloud Network Insights from the monitored Peer. If the number of advertised prefixes falls below the minimum number that is expected, it indicates a problem with the peering session between the monitored peer and Crosswork Cloud Network Insights or any of its other peers. It can also be caused by a more restrictive inbound policy configured on the monitored peer applied to its peers other than Crosswork Cloud Network Insights or a more restrictive outbound policy applied to the Crosswork Cloud Network Insights peer. Conversely, if the number of advertised prefixes exceeds the maximum number that is expected, it can indicate less restrictive policies configured or a malicious attempt to overwhelm the peer with prefix advertisements.

Possible Problem Detected

This alarm can help identify problems with peering (because of software, hardware, or misconfiguration issues) or DoS attacks on the peer.

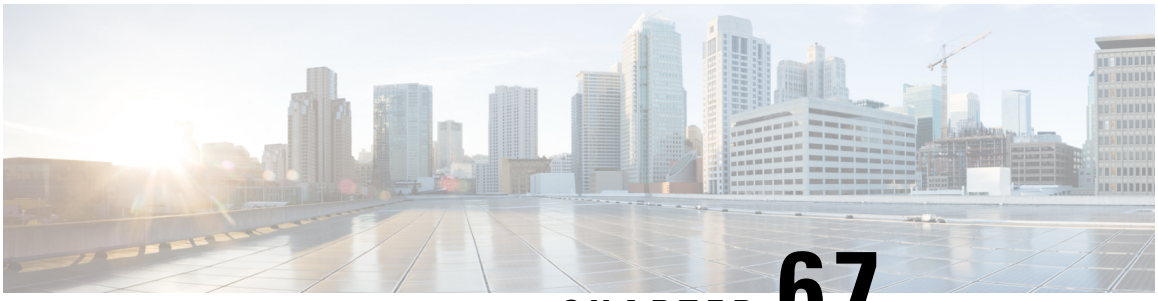
Relevant Alarm Rule Configurations

The following options must be configured when adding this alarm rule to an ASN policy configuration (**External Routing Analysis > Configure > Policies > Add Policy > Peer Policy > Add Rule > Advertised Prefix Count**):

- Expected prefix count range (per IPv4/IPv6 address family)

Example

You create a Peer Policy with the **Advertised Prefix Count** alarm rule with an expected IPv4 prefix range [1000, 800000] and linked to Peer RTR1. The alarm activates at every data collection event if the number of IPv4 prefixes advertised from RTR1 to Crosswork Cloud Network Insights is outside this range, and different than what was previously recorded.



CHAPTER 67

Prohibited IP Prefix

Prohibited IP Prefix

This alarm detects if a monitored peer has a prohibited prefix in the public IP routing space installed in its Routing Information Base (RIB) or the monitored peer is forwarding it.

Bogons are IP address blocks that are not public, either because they are reserved or have not been allocated to a Regional Internet Registry (RIR). *Full bogons* also include address blocks that have been assigned to the RIRs but are not allocated by the RIR to a specific network. It is good practice for routers to filter advertisements for a prohibited prefix. A user can choose to be alerted only for bogon advertisements using this alarm.

Possible Problem Detected

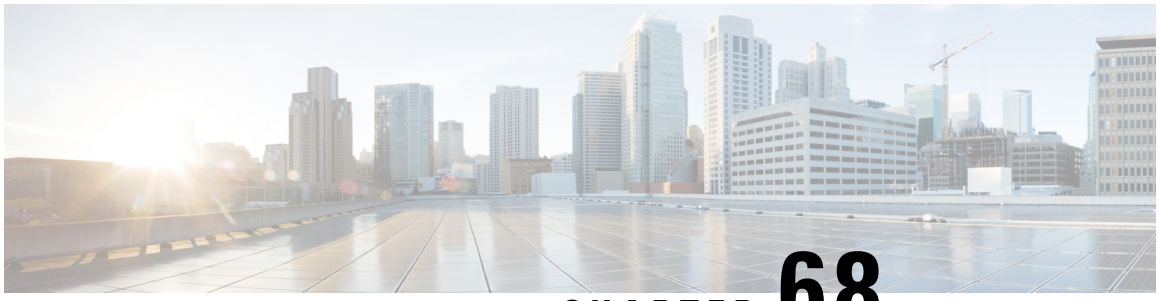
This alarm can help identify DoS attacks on routers.

Relevant Alarm Rule Configurations

Select **Bogons** or **Full Bogons** when adding this alarm rule to a Peer policy configuration (**External Routing Analysis > Configure > Policies > Add Policy > Peer Policy > Add Rule > Prohibited IP Prefix**).

Example

You create a Peer Policy with the **Prohibited IP Prefix** alarm rule with option **Bogons** and linked to Peer RTR1. The alarm activates when RTR1 advertises 10.0.0.0/24 (Bogon per RFC1918) to Crosswork Cloud Network Insights but not when 2001:221::/32 (Full Bogon) is advertised.



CHAPTER 68

Gateway Connectivity

Gateway Connectivity

After a Crosswork Data Gateway is installed for Crosswork Cloud Traffic Analysis or Crosswork Cloud Trust Insights, a policy is automatically created to monitor the connection between Crosswork Data Gateway and Crosswork Cloud. If the Crosswork Data Gateway loses connection to Crosswork Cloud (fails to communicate with Crosswork Cloud within its reporting interval), an alarm is generated and displayed in the Alarms page (or > **Monitor** > **Alarms**).

To view gateway connectivity details or to update the alarm severity level, list of monitored gateways, or notification endpoints, do the following:

Step 1 Navigate to or > **Configure** > **Policies.**

Under **Gateway Connectivity**, you can view the number of active alarms, the number of gateways monitored, and the gateway that has the most recent active alarm.

Step 2 Under **Gateway Connectivity**, click **Details**.

Step 3 By default, the **Overview** tab displays the current gateway connectivity policy configuration.

Step 4 To view Alarm details, click the **Alarms** tab. From this page, you can click the **Lost Gateway Connection** alarm for further details about a particular alarm or navigate between the Active, Acknowledge, or History tabs.

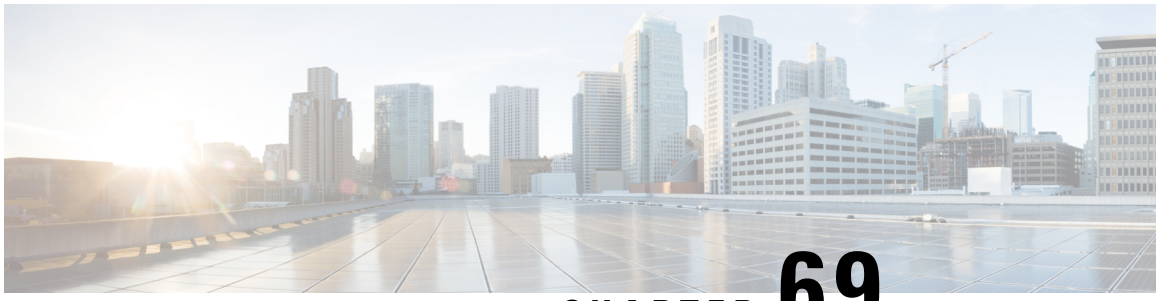
Step 5 To modify the alarm severity, list of monitored gateways, or configure endpoint notifications, click **Edit**.

a) Under **Triggers** > **Gateway Rules** > **Severity** drop-down menu, select the severity level.

b) Under **Data**, click **Modify** to update which gateways you want to monitor or ignore.

c) Under **Actions**, you can either modify existing endpoint notifications or add more. For more information on the types of endpoint notifications you can configure, see About Notification Endpoints, on page 87.

d) Click **Save**.



CHAPTER 69

Device Connectivity

Device Connectivity

After a device is linked to the Crosswork Data Gateway and added to Crosswork Cloud Traffic Analysis or Crosswork Cloud Trust Insights, a policy is automatically created to monitor the connection between the Crosswork Data Gateway and the device. If the Crosswork Data Gateway loses connection with the device, an alarm is generated and displayed in the **Alarms** page (**> Monitor > Alarms**).

To view device connectivity details or update the severity level, list of monitored devices, or notification endpoints, do the following:

Step 1 Navigate to or **> Configure > Policies.**

Under **Device Connectivity**, you can view the number of active alarms, number of devices monitored, and the device that has the most recent active alarm.

Step 2 Under **Device Connectivity**, click **Details**.

Step 3 By default, the **Overview** tab displays the current device connectivity policy configuration.

Step 4 To view Alarm details, click the **Alarms** tab. From this page, you can click the **Lost Device Connection** alarm for further details about that particular alarm or navigate between the Active, Acknowledge, or History tabs.

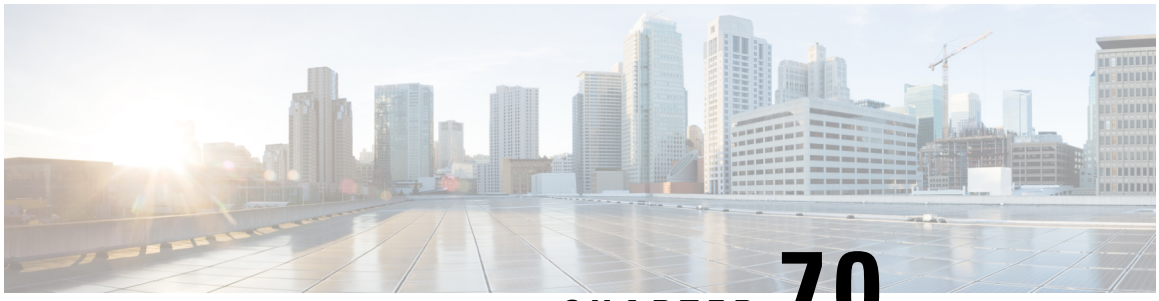
Step 5 To modify the alarm severity, list of monitored devices, or configure endpoint notifications, click **Edit**.

a) Under **Triggers > Device Rules > Severity** drop-down menu, select the severity level.

b) Under **Data**, click **Modify** to update which devices you want to monitor or ignore.

c) Under **Actions**, you can either modify existing endpoint notifications or add more. For more information on the types of endpoint notifications you can configure, see About Notification Endpoints, on page 87.

d) Click **Save**.



CHAPTER 70

Interface TX Utilization

Interface TX Utilization

This alarm monitors transmitting traffic information and is triggered when interface TX utilization is outside the range you specify. To configure this alarm, do the following:

Step 1 In the main window, click > **Configure** > **Policies**.

Step 2 Click **Add Policy**.

Step 3 Enter a policy name in the **Name** field.

Step 4 Under **Triggers**, click **Add Rules**.

Step 5 Click **Interface TX Utilization**.

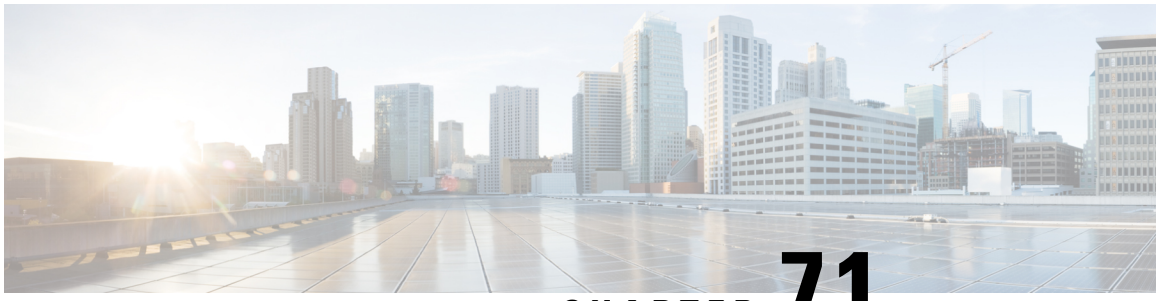
Step 6 Click **Next**.

Step 7 By default, the rule is enabled. Toggle the switch to DISABLED if you do not want to activate the rule yet.

Step 8 Use the slider to indicate utilization ranges that will trigger this alarm. Crosswork Cloud will send a notification if utilization is within the range indicated by the color red and ALARM text.

Step 9 Under the **Severity** drop-down list, select the severity level you want defined for this alarm.

Step 10 Make any other necessary interface and endpoint notification configurations, then click **Save**.



CHAPTER 71

Interface RX Utilization

Interface RX Utilization

This alarm monitors receiving traffic information and is triggered when interface RX utilization is outside the range you specify. To configure this alarm, do the following:

Step 1 In the main window, click > **Configure** > **Policies**.

Step 2 Click **Add Policy**.

Step 3 Enter a policy name in the **Name** field.

Step 4 Under **Triggers**, click **Add Rules**.

Step 5 Click **Interface RX Utilization**.

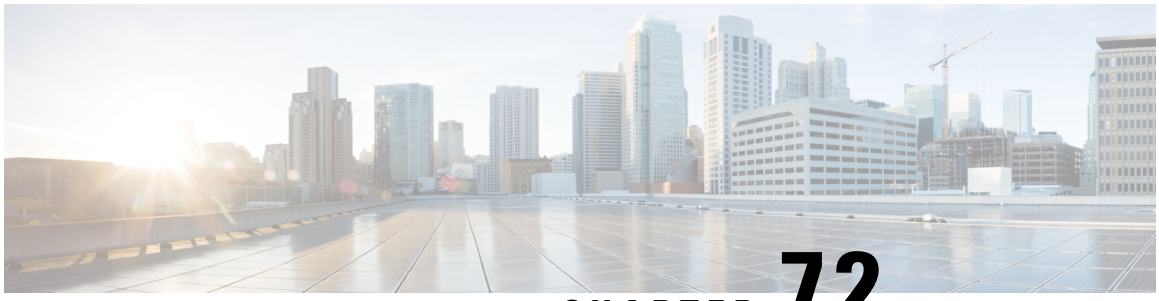
Step 6 Click **Next**.

Step 7 By default, the rule is enabled. Toggle the switch to DISABLED if you do not want to activate the rule yet.

Step 8 Use the slider to indicate utilization ranges that will trigger this alarm. Crosswork Cloud will send a notification if utilization is within the range indicated by the color red and ALARM text.

Step 9 Under the **Severity** drop-down list, select the severity level you want defined for this alarm.

Step 10 Make any other necessary interface and endpoint notification configurations, then click **Save**.



CHAPTER 72

Prefix Utilization

Prefix Utilization

This alarm monitors the capacity of a prefix and is triggered when the maximum percentage of total capacity of a single prefix on a monitored interface is exceeded. To configure this alarm, do the following:

Step 1 In the main window, click > **Configure** > **Policies**.

Step 2 Click **Add Policy**.

Step 3 Enter a policy name in the **Name** field.

Step 4 Under **Triggers**, click **Add Rules**.

Step 5 Click **Prefix Utilization**.

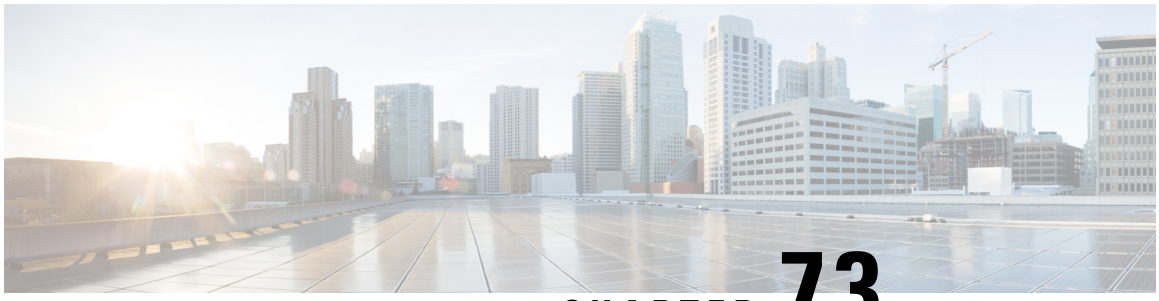
Step 6 Click **Next**.

Step 7 By default, the rule is enabled. Toggle the switch to DISABLED if you do not want to activate the rule yet.

Step 8 Use the slider to indicate the utilization range that will trigger this alarm. Crosswork Cloud will send a notification if utilization is within the range indicated by the color red and ALARM text.

Step 9 Under the **Severity** drop-down list, select the severity level you want defined for this alarm.

Step 10 Make any other necessary interface and endpoint notification configurations, then click **Save**.



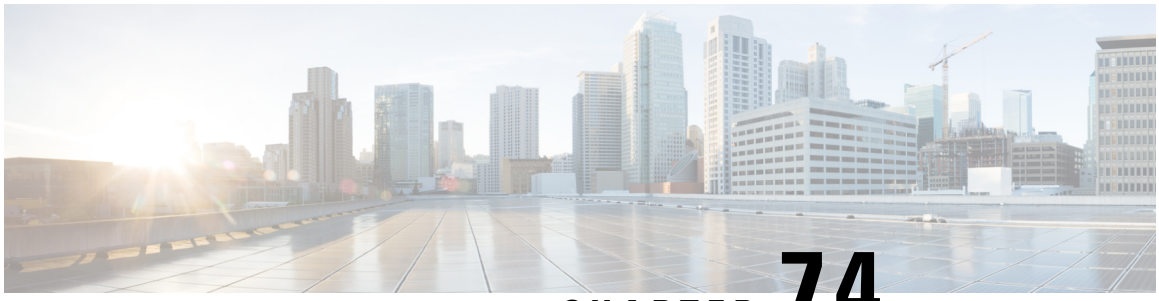
CHAPTER 73

Device Certificate Expiring

Device Certificate Expiring

This alarm monitors pending device certificate expiration and is triggered when the amount of days prior to expiration reaches the time you specify (7, 30, 60 or 90 days). To configure this alarm, do the following:

Step 1 In the main window, click > **Configure** > **Policies**.
Step 2 Click **Add Policy**.
Step 3 Enter a policy name in the **Name** field.
Step 4 Under **Triggers**, click **Add Rules**.
Step 5 Click **Device Certificate Expiring**.
Step 6 Click **Next**.
Step 7 By default, the rule is enabled. Toggle the switch to DISABLED if you do not want to activate the rule yet.
Step 8 Choose the expiration status required to trigger the alarm.
Step 9 Under the **Severity** drop-down list, select the severity level you want defined for this alarm.
Step 10 Make any other necessary interface and endpoint notification configurations, then click **Save**.



CHAPTER 74

Device Certificate Violation

Device Certificate Violation

This alarm is triggered when the device certificate used to sign the dossier from the device does not match the device enrollment certificate on record in Crosswork Cloud. To clear the alarm, review and accept the new enrollment device certificate in the UI. To configure this alarm, do the following:

Step 1 In the main window, click > **Configure** > **Policies**.

Step 2 Click **Add Policy**.

Step 3 Enter a policy name in the **Name** field.

Step 4 Under **Triggers**, click **Add Rules**.

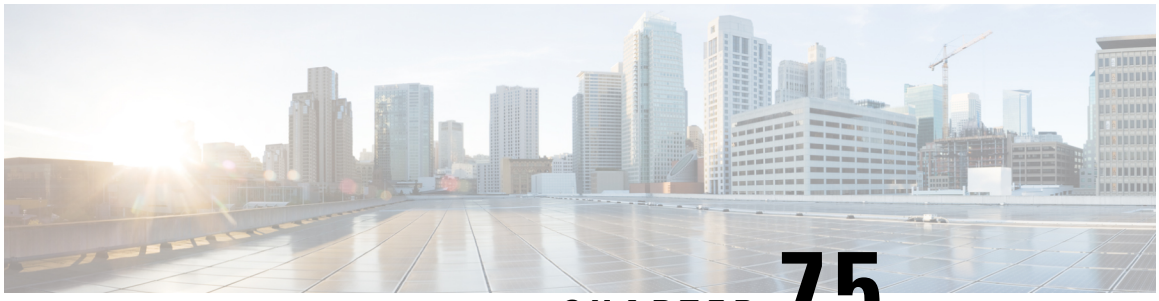
Step 5 Click **Device Enrollment Certificate Violation**.

Step 6 Click **Next**.

Step 7 By default, the rule is enabled. Toggle the switch to DISABLED if you do not want to activate the rule yet.

Step 8 Under the **Severity** drop-down list, select the severity level you want defined for this alarm.

Step 9 Make any other necessary interface and endpoint notification configurations, then click **Save**.



CHAPTER 75

Device Running Configuration Change

Device Running Configuration Change

This alarm monitors possible unwanted device configuration changes. Crosswork Trust Insights checks to see if the stored hash does not match the hash reported by the system. If the hashes do not match, then a device configuration change has occurred.

Before you begin

Hash configuration collection on the device must be enabled (**Devices** > ***device-name*** > **Edit**).

Step 1 In the main window, click > **Configure** > **Policies**.

Step 2 Click **Add Policy**.

Step 3 Enter a policy name in the **Name** field.

Step 4 Under **Triggers**, click **Add Rules**.

Step 5 Click **Device Running Configuration Change**.

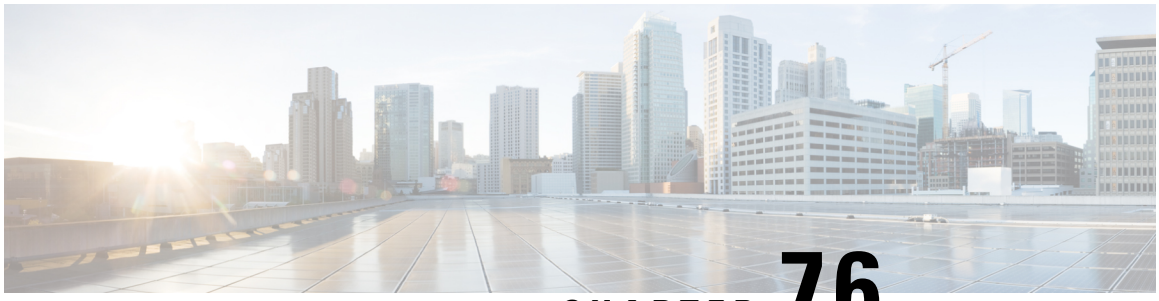
Step 6 Click **Next**.

Step 7 By default, the rule is enabled. Toggle the switch to DISABLED if you do not want to activate the rule yet.

Step 8 Under the **Severity** drop-down list, select the severity level you want defined for this alarm.

Step 9 Click **Next**.

Step 10 Make any other necessary configurations, then click **Save**.



CHAPTER 76

Device SSH Host Key Violation

Device SSH Host Key Violation

This alarm is triggered when the device SSH host key has changed and does not match the SSH host key on record in Crosswork Cloud for the device. To clear this alarm, verify and accept the new SSH keys via the UI. To configure this alarm, do the following:

Step 1 In the main window, click > **Configure** > **Policies**.

Step 2 Click **Add Policy**.

Step 3 Enter a policy name in the **Name** field.

Step 4 Under **Triggers**, click **Add Rules**.

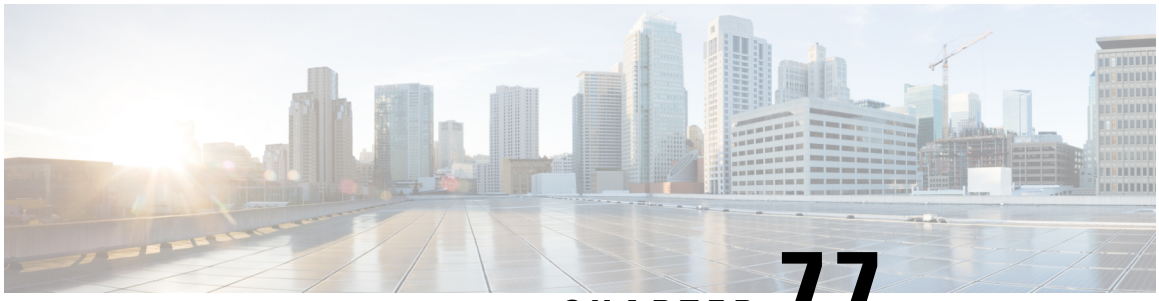
Step 5 Click **Device SSH Host Key Violation**.

Step 6 Click **Next**.

Step 7 By default, the rule is enabled. Toggle the switch to DISABLED if you do not want to activate the rule yet.

Step 8 Under the **Severity** drop-down list, select the severity level you want defined for this alarm.

Step 9 Make any other necessary interface and endpoint notification configurations, then click **Save**.



CHAPTER 77

Dossier Collection Failure

Dossier Collection Failure

This alarm is triggered when there is a failure collecting a dossier from a monitored Cisco IOS XR device. To configure this alarm, do the following:

Step 1 In the main window, click > **Configure** > **Policies**.

Step 2 Click **Add Policy**.

Step 3 Enter a policy name in the **Name** field.

Step 4 Under **Triggers**, click **Add Rules**.

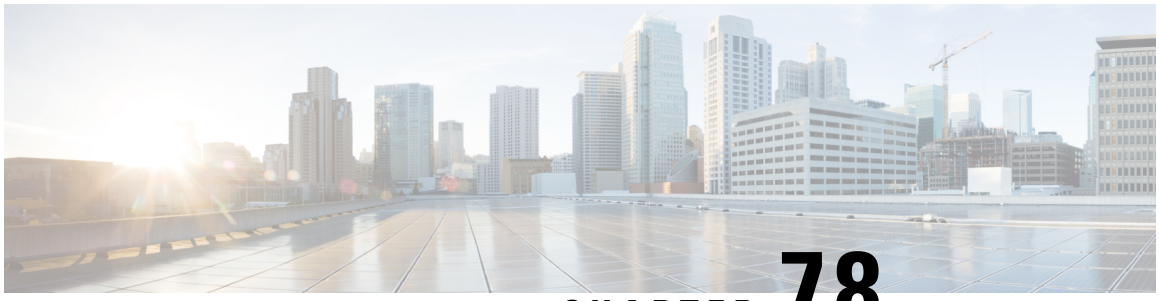
Step 5 Click **Dossier Collection Failure**.

Step 6 Click **Next**.

Step 7 By default, the rule is enabled. Toggle the switch to DISABLED if you do not want to activate the rule yet.

Step 8 Under the **Severity** drop-down list, select the severity level you want defined for this alarm.

Step 9 Make any other necessary interface and endpoint notification configurations, then click **Save**.



CHAPTER 78

Expired Device Certificate

Expired Device Certificate

This alarm is triggered when the certificate used to enroll the monitored device has expired. To clear the alarm, generate a new enrollment certificate, then review and accept it in the UI. To configure this alarm, do the following:

Step 1 In the main window, click > **Configure** > **Policies**.

Step 2 Click **Add Policy**.

Step 3 Enter a policy name in the **Name** field.

Step 4 Under **Triggers**, click **Add Rules**.

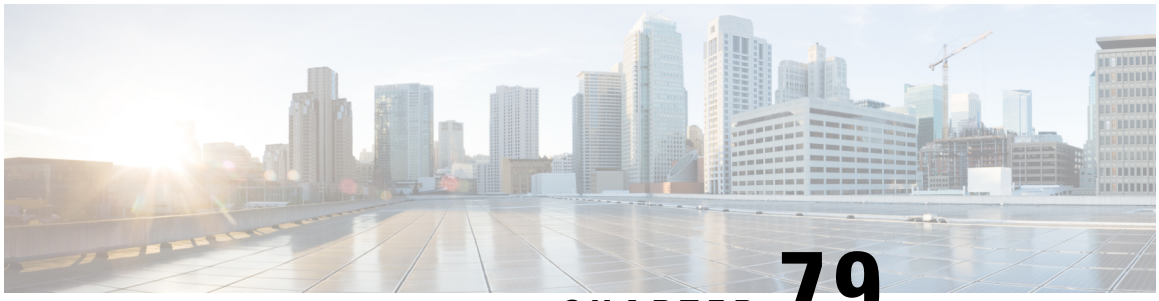
Step 5 Click **Expired Device Certificate**.

Step 6 Click **Next**.

Step 7 By default, the rule is enabled. Toggle the switch to DISABLED if you do not want to activate the rule yet.

Step 8 Under the **Severity** drop-down list, select the severity level you want defined for this alarm.

Step 9 Make any other necessary interface and endpoint notification configurations, then click **Save**.



CHAPTER 79

Hardware Integrity Validation

Hardware Integrity Validation

This alarm monitors the number of Cisco Secure Unique Device Identifier (SUDI) certificate failures. The SUDI can be used as an unchangeable device identity for configuration, security, auditing, and management. It enables accurate, consistent, and electronic identification of Cisco products for asset management, provisioning, version visibility, service entitlement, quality feedback, and inventory management.

You specify the number of SUDI failures that will trigger an alarm. To configure this alarm, do the following:

Step 1 In the main window, click > **Configure** > **Policies**.

Step 2 Click **Add Policy**.

Step 3 Enter a policy name in the **Name** field.

Step 4 Under **Triggers**, click **Add Rules**.

Step 5 Click **Hardware Integrity Validation**.

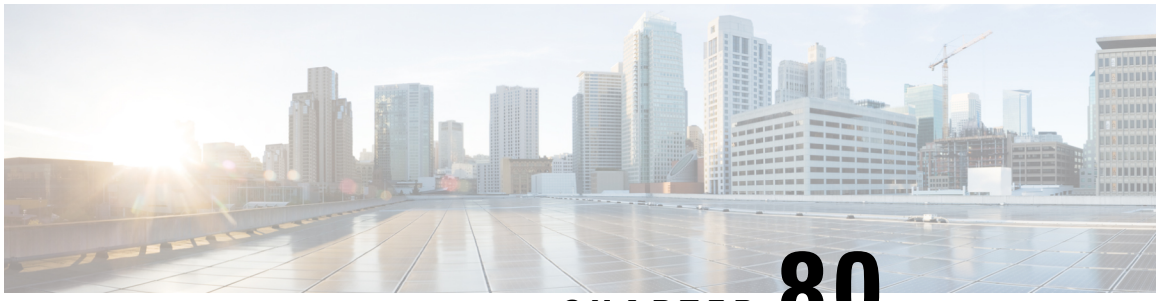
Step 6 Click **Next**.

Step 7 By default, the rule is enabled. Toggle the switch to DISABLED if you do not want to activate the rule yet.

Step 8 Use the slider to indicate the number of SUDI failures that will trigger this alarm.

Step 9 Under the **Severity** drop-down list, select the severity level you want defined for this alarm.

Step 10 Make any other necessary interface and endpoint notification configurations, then click **Save**.



CHAPTER 80

Mismatched Files

Mismatched Files

This alarm monitors the integrity of the software artifacts and files running on the device by verifying their hashes against the Known Good Values (KGVs) for the version of software running on the device. You can configure the number of mismatches that would trigger an alarm. To address mismatched files, you can investigate the device and look at which Cisco IOS XR version is running, who last deployed the file, where the file came from, and so on. To configure this alarm, do the following:

Step 1 In the main window, click > **Configure** > **Policies**.

Step 2 Click **Add Policy**.

Step 3 Enter a policy name in the **Name** field.

Step 4 Under **Triggers**, click **Add Rules**.

Step 5 Click **Mismatched Files**.

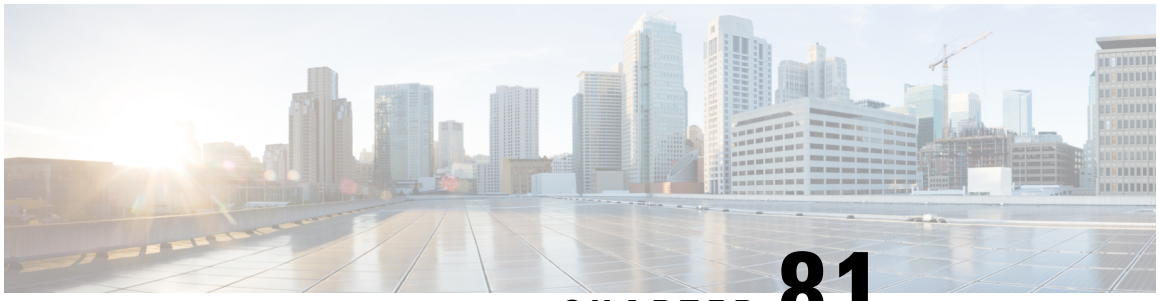
Step 6 Click **Next**.

Step 7 By default, the rule is enabled. Toggle the switch to DISABLED if you do not want to activate the rule yet.

Step 8 Use the slider to indicate the number of mismatched files that will trigger this alarm. Crosswork Cloud will send a notification if the number of mismatched files is within the range indicated by the color red and ALARM text.

Step 9 Under the **Severity** drop-down list, select the severity level you want defined for this alarm.

Step 10 Make any other necessary interface and endpoint notification configurations, then click **Save**.



CHAPTER 81

Package Validation

Package Validation

This alarm detects software packages (or files within those packages) that have unknown installation or running signatures. To configure this alarm, do the following:

Step 1 In the main window, click > **Configure** > **Policies**.

Step 2 Click **Add Policy**.

Step 3 Enter a policy name in the **Name** field.

Step 4 Under **Triggers**, click **Add Rules**.

Step 5 Click **Package Validation**.

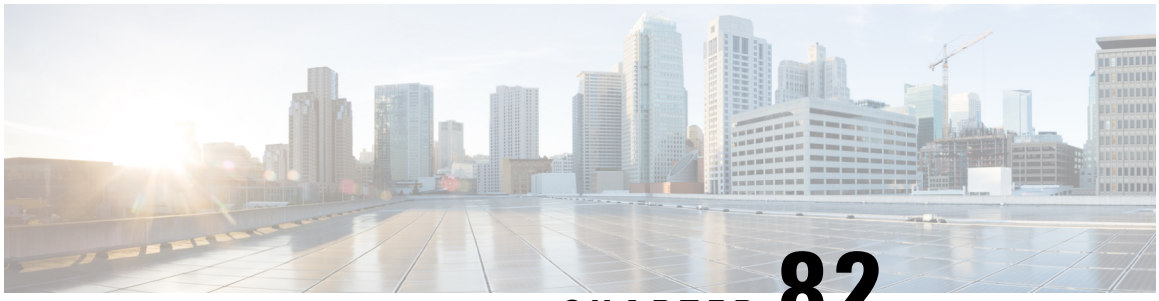
Step 6 Click **Next**.

Step 7 By default, the rule is enabled. Toggle the switch to DISABLED if you do not want to activate the rule yet.

Step 8 Use the slider to indicate the number of software integrity failures that will trigger this alarm. Crosswork Cloud will send a notification if the number of failures is within the range indicated by the color red and ALARM text.

Step 9 Under the **Severity** drop-down list, select the severity level you want defined for this alarm.

Step 10 Make any other necessary interface and endpoint notification configurations, then click **Save**.



CHAPTER 82

Unknown Files

Unknown Files

This alarm monitors the number of unknown files that do not match known Cisco IOS XR Known Good Values (KGV) or user defined KGVs . You specify the number of unknown files that will trigger an alarm. To clear the alarm, mark the files as "known" to add them to the Known Good Values list.

Step 1 In the main window, click > **Configure** > **Policies**.

Step 2 Click **Add Policy**.

Step 3 Enter a policy name in the **Name** field.

Step 4 Under **Triggers**, click **Add Rules**.

Step 5 Click **Unknown Files**.

Step 6 Click **Next**.

Step 7 By default, the rule is enabled. Toggle the switch to DISABLED if you do not want to activate the rule yet.

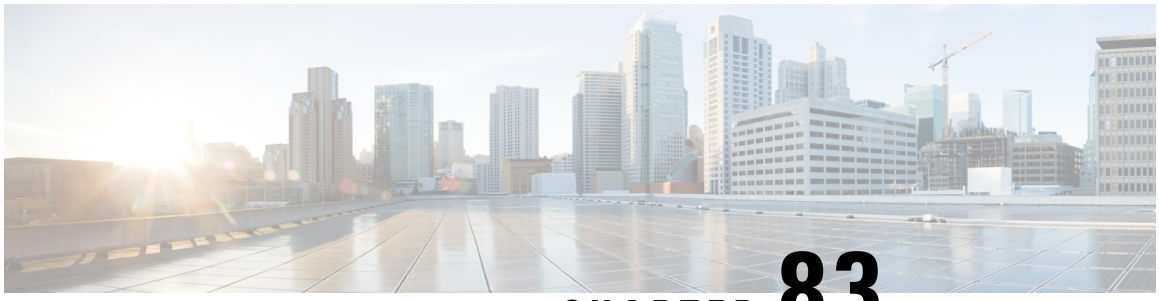
Step 8 Use the slider to indicate the number of unknown files that will trigger this alarm. Crosswork Cloud will send a notification if the number of unknown files is within the range indicated by the color red and ALARM text.

Step 9 Under the **Severity** drop-down list, select the severity level you want defined for this alarm.

Step 10 Make any other necessary interface and endpoint notification configurations, then click **Save**.

PART XII

About Alarms



CHAPTER 83

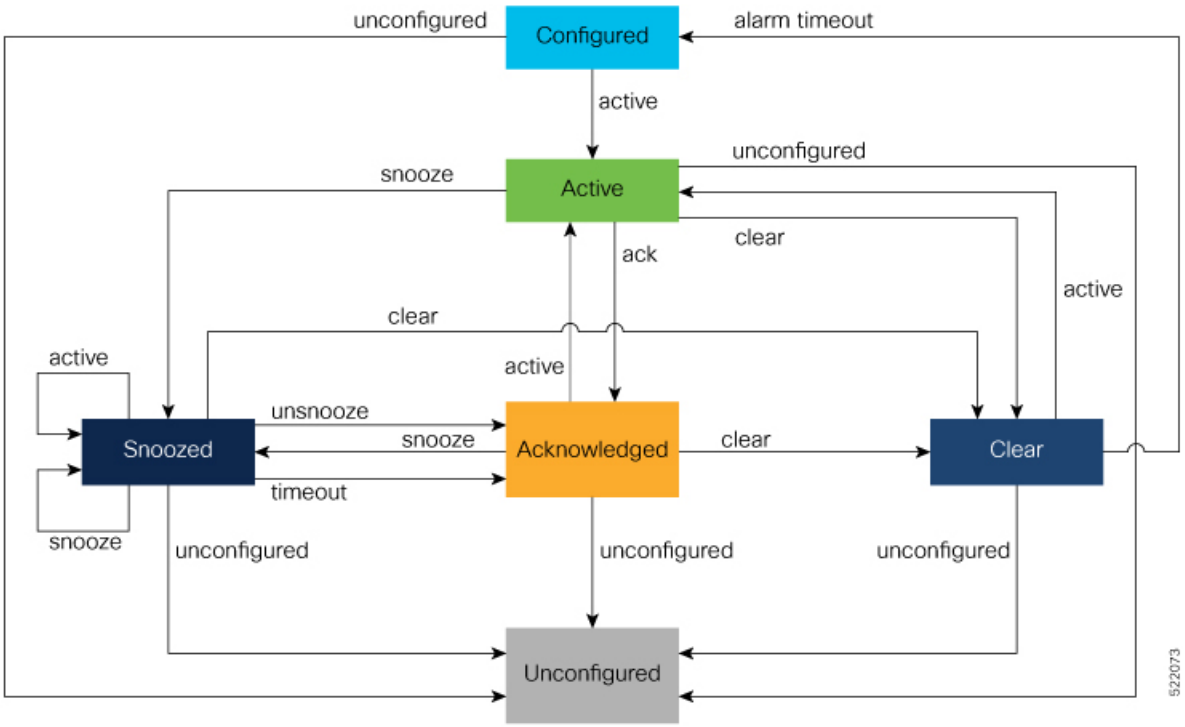
Alarm Lifecycle

Crosswork Cloud creates an alarm instance for each rule in a fully configured alarm policy. A fully configured alarm policy has one or more rules and depending on the alarm policy type, has one or more prefixes, ASNs, or peers associated with it.

Each alarm instance has a lifecycle, transitioning between various states after it is created. The following diagram shows what transitions can occur from each state. For more information, see Alarm States, on page 356.

Note Each alarm instance starts its lifecycle in a **Configured** state.

Figure 11: Alarm Lifecycle



- Alarm States, on page 356

Alarm States

An alarm instance transitions between the states in response to events or in response to a user action.

The following table describes the possible alarm states.

Table 37: Alarm State Descriptions

Alarm Status	Description
Configured	Initial state of an alarm.
Active	The state when an alarm is triggered with an active event.
Acknowledged	In this state, a user has indicated the alarm is recognized and acknowledged. An alarm that is in **Active** or **Snoozed** state can be marked as acknowledged. **Note** • An alarm in the **Acknowledged** state will not show up in the list of active alarms. • An alarm in the **Acknowledged** state will transition back to **Active** state, if there is another active alert.
Clear	The alarm is no longer active. The **Clear** state is an ephemeral state. The alarm instance transitions to a configured state after a 30 second hold time.
Snoozed	An alarm that is in **Active** or **Acknowledged** state can be marked as **Snoozed** by the user for a specified time period. During this period, the alarm shows up in the active alarms list. However, if the alarm condition clears, then a notification will be sent to the notification endpoint (if one was configured).
Active (Snoozed)	The alarm has been **Snoozed**, but the conditions that would trigger the alarm to be **Active** are present.
Cleared (Snoozed)	The alarm has been **Snoozed** and the conditions that would trigger the alarm are no longer present.
Unconfigured	An alarm transitions to an **Unconfigured** state and is eventually deleted when the user deletes the alarm policy, or the rule corresponding to the alarm instance. The **Unconfigured** state is an ephemeral state, and the alarm instance is deleted after a 30 second hold time.

Note

• An alarm instance can transition to an **Active** or **Clear** state, only in response to an event received from the alarm detection layer.

Alarm Notifications

When a policy rule is violated, you can configure an alarm notification to be sent to one or more endpoints (see Configure Notification Endpoints, on page 88). The notification contains information about the alarm state and alarm event data.

Notifications are sent if one of the following alarm state changes occur:

- From Active to Clear
- From Configured to Active
- From Acknowledged to Clear
- From Snoozed to Clear

A notification will not be generated if an alarm becomes active again *and* is already in one of the following states:

- Active
- Snoozed
- Acknowledged

Related Links

- About Notification Endpoints, on page 87

Crosswork Network Insights Alarm Types

Alarms are categorized into three types:

Type	Description
ASN	Autonomous System Number (ASN) type alarms monitor the state of a configured BGP Autonomous System (AS). These alarms are generally used to detect unexpected prefixes coming from your ASN and alert you if an expected condition is violated. For example, an alarm becomes active if Crosswork Cloud Network Insights detects a new prefix that was not previously observed and should not be originating from a configured ASN.
PEER	Peer type alarms monitor the state of a configured Peer and its Routing Information Base (RIB). These alarms are used when you have configured peer monitoring. For example, an alarm becomes active if Crosswork Cloud Network Insights detects a number of prefixes in RIB that is outside the configured parameters.
PREFIX	Prefix type alarms monitor the state of a configured prefix and a number of its BGP attributes, such as the Origin ASN of the prefix or the length of the AS path attribute. It is the most common alarm type and is designed to detect unknown events on prefixes that are being monitored. A set of prefix type alarms also monitor the ROA status (VALID, INVALID or ABOUT-TO-EXPIRE) of the configured prefix.

Alarm Thresholds

Alarm thresholds are used to control the sensitivity of alarms. Consider configuring alarm thresholds if some alarms are often being triggered by small numbers of observed changes and are considered "false alarms".

An alarm is triggered (Active) when Crosswork Cloud Network Insights detects a violation against a set of conditions related to a monitored AS, peer, or prefix. The alarm clears when all conditions are no longer violated. Since data is collected from many BGP Peers, Crosswork Cloud Network Insights has access to multiple views of the state of a prefix or AS. These views are not always identical, and the frequent state changes in a small number of peers (such as those caused by router flap) can produce a lot of alarm noise. Thresholds can act as a noise dampening mechanism.

The following Peer Count thresholds can be configured for certain alarm rules to dampen alarm noise:

Peers to Trigger—The minimum number of violation peers required to report a condition violation that would cause the alarm to become Active. For example: A **Peers to Trigger** threshold has been set to 1 for the Prefix Withdrawal alarm. The number of peers reporting that a prefix has been withdrawn has to exceed 1 before External Routing Analysis issues an Active prefix withdrawal alarm.

Peers to Resolve—After an alarm has been activated, it remains Active. The alarm is triggered again with every new condition violation until the violation peer count is less than or equal to the **Peers to Resolve** threshold (for example, this can occur due to the withdrawal of violating advertisements or an increase to the Peers to Resolve threshold). The alarm then goes into Clear state.

Note The **Peers to Resolve** threshold must be less than the **Peers to Trigger** threshold.

Figure 12: Example: Expected AS Path Alarm Rule Threshold Options