View Alarm Descriptions

Alarm descriptions

These tables allow you to quickly view all Crosswork Cloud alarms by application. To view a description of a specific alarm, click an alarm from the appropriate application table.

Table 1: Crosswork Cloud Network Insights Alarms

Unexpected AS Prefix	Prefix Withdrawal	Upstream AS Change
AS Origin Violation	ROA Expiry	Valid AS Path Violation
New AS Path Edge	ROA Failure	Peer Down
AS Path Length Violation	ROA Not Found	Advertised Prefix Count
Parent Aggregate Change	DNS Root Prefix Withdrawal	Prohibited IP Prefix
Prefix Advertisement	Subprefix Advertisement	

Table 2: Crosswork Cloud Traffic Analysis Alarms

Gateway Connectivity	Device Connectivity	Interface TX Utilization
Interface RX Utilization	Prefix Utilization	

Table 3: Crosswork Cloud Trust Insights Alarms

Gateway Connectivity	Device Running Configuration Change	Hardware Integrity Validation
Device Connectivity	Device SSH Host Key Violation	Mismatched Files

Device Certificate Expiring	Dossier Collection Failure	Package Validation
Device Certificate Violation	Expired Device Certificate	Unknown Files

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). 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

Alarm types for Crosswork Network Insights

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.

Type	Description
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 for Crosswork Cloud Network Insights

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.

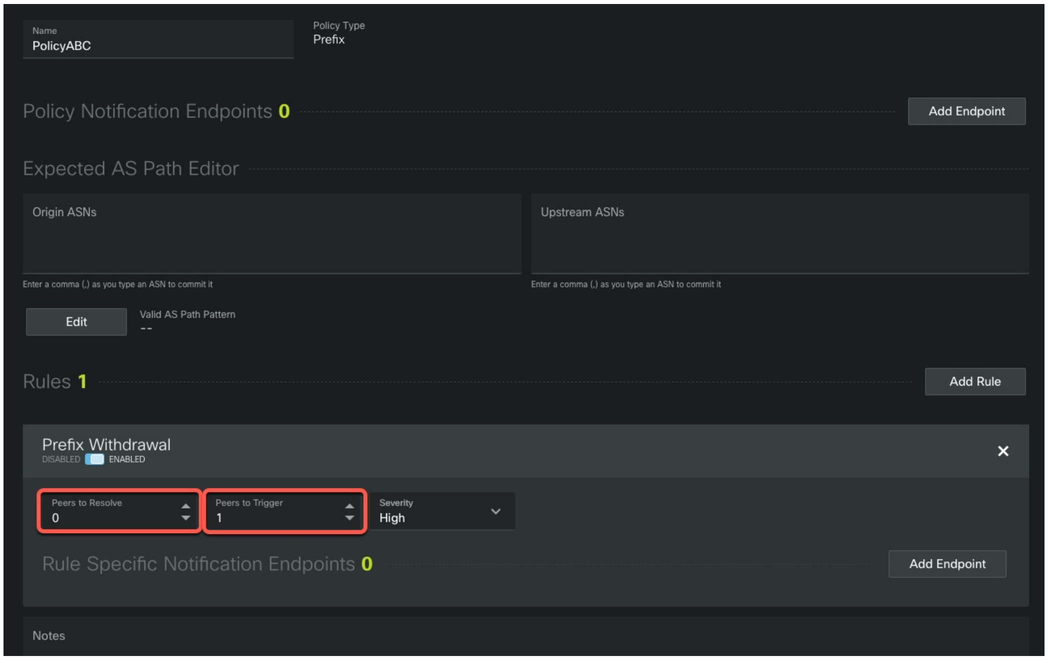
The following Peer Count thresholds can be configured for certain alarm rules to dampen alarm noise:

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 1: Example: Expected AS Path Alarm Rule Threshold Options



Name: PolicyABC

Policy Type: Prefix

Policy Notification Endpoints 0

Expected AS Path Editor

Origin ASNs

Enter a comma (,) as you type an ASN to commit it

Upstream ASNs

Enter a comma (,) as you type an ASN to commit it

Valid AS Path Pattern: --

Rules 1

Prefix Withdrawal

DISABLED ENABLED

Peers to Resolve: 0

Peers to Trigger: 1

Severity: High

Rule Specific Notification Endpoints 0

Notes