

Configure Peers

- Import peers, on page 1
- Add peers, on page 2
- View peer details, on page 2
- Configure peer devices, on page 4
- Edit peers, on page 6
- Disable peers, on page 6
- Remove peers, on page 7

Import peers

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

Procedure

Step 1 Choose **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.

Procedure

Step 1 Choose **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 2.

Step 6 Configure the peer device. For more information, see Configure peer devices, on page 4.

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 4).

Procedure

Step 1 Choose **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, disable, or remove this peer by clicking on the corresponding button.

Table 1: Overview

Field	Description
Linked Policy	The policy associated with the prefix.
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 4.
Number of Prefixes	A 7-day timeline that displays the average number of prefixes that are accepted by your peer.

Table 2: 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.

Field	Description
Severity	The configured severity level of the alarm.
Activated	Date and time the alarm occurred.

Table 3: BGP Updates

Field	Description
Timeframe	Specify a timeframe by selecting a value from the **Timeframe** drop-down list.
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 2 and View peer details, on page 2.

- <*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 2 and View peer details, on page 2.

- <*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.

Procedure

Step 1 Choose **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 7.

Procedure

Step 1 Choose **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 6.

Procedure

Step 1 Choose **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.