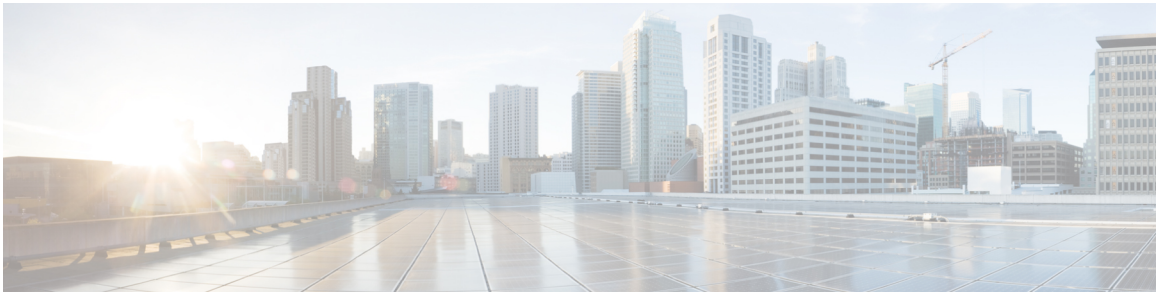
Cisco Crosswork Cloud Quick Start Guide

First Published: 2023-05-03

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



CONTENTS

CHAPTER 1 **Overview** 1

About Crosswork Cloud Network Insights 1

About Traffic Analysis 2

About Trust Insights 3

About Cisco Crosswork Data Gateway 3

CHAPTER 2 **Set Up Crosswork Cloud** 5

Log In 5

Add Users 5

Set Up the Organization Tenancy 6

CHAPTER 3 **Get Started with Crosswork Cloud Network Insights** 7

Get Started with Crosswork Cloud Network Insights 7

CHAPTER 4 **Get Started with Crosswork Cloud Traffic Analysis** 11

Get Started with Crosswork Cloud Traffic Analysis 11

CHAPTER 5 **Get Started with Crosswork Cloud Trust Insights** 15

Get Started with Crosswork Cloud Trust Insights 15

CHAPTER 6 **Troubleshoot Crosswork Cloud** 19

Troubleshoot Crosswork Data Gateway Connectivity 19

CHAPTER 7 **Subscription Plans** 21

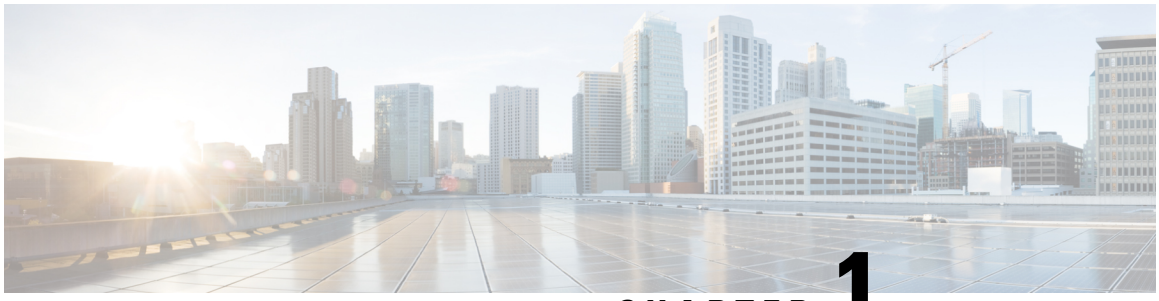
View Subscription Plan Options 21

Free Subscription Plan Requirement 21

CHAPTER 8 Supplemental Information 23

Install Crosswork Data Gateway Using vCenter vSphere Client 23

?



CHAPTER 1

Overview

This document provides a high-level description of the steps that are required to set up and start using Cisco Crosswork Cloud.

- About Crosswork Cloud Network Insights, on page 1
- About Traffic Analysis, on page 2
- About Trust Insights, on page 3
- About Cisco Crosswork Data Gateway, on page 3

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.

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.

About Trust Insights

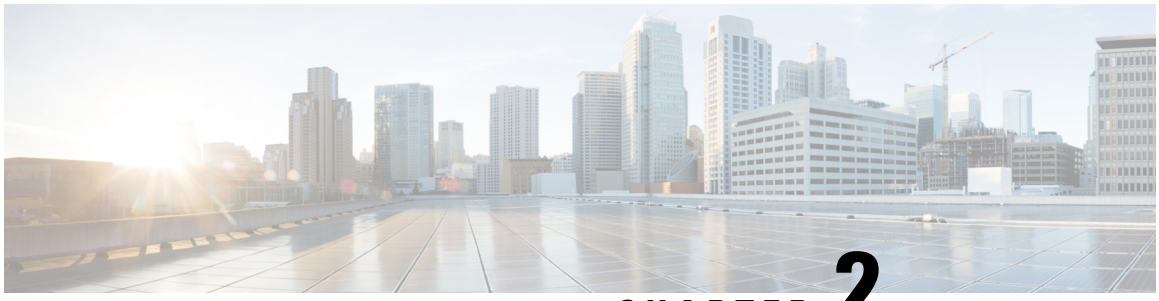
Crosswork Cloud Trust Insights provides a way to protect and test the integrity of Cisco IOS XR devices on your network. Crosswork Cloud Trust Insights gathers secure measurements and proves that the data was collected at a certain time, which allows you to measure, verify, and audit the integrity of 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?

About Cisco Crosswork Data Gateway

Crosswork Data Gateway is designed as an easy to deploy and maintain gateway within customer networks to facilitate secure collection of data from devices, without requiring direct connectivity to external cloud resources. Crosswork Data Gateway is designed for streamlined deployment in common virtualization environments like Vmware ESXi, and once deployed is completely managed by the Crosswork Cloud service. This is designed to minimize the operational and maintenance requirements of deploying and managing Crosswork Cloud applications. Since Crosswork Cloud can manage multiple Cloud Data Gateways, Crosswork Cloud Traffic Analysis and Crosswork Cloud Trust Insights can easily support scalable deployments of peering traffic data and trust evidence collection from large production networks with easy geographical separation of collection, and minimal cost of management.



CHAPTER 2

Set Up Crosswork Cloud

This section describes the initial steps to do when using Crosswork Cloud for the first time:

- Log In, on page 5
- Add Users, on page 5
- Set Up the Organization Tenancy, on page 6

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:

Procedure

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.

Add Users

If you have admin privileges you can add users that have a Cisco.com account.

Procedure

Step 1 In the main window, click > **Users** > **Add User**.

Step 2 Toggle selection to **Enabled** (default). Disabled users can't log in.

Step 3 Enter one or more user email addresses (specified in their Cisco.com user profile) separated by a space, comma, or semicolon.

Step 4 Under the **Role** drop-down menu, select the user's access. For more information, see User Roles.

Step 5 Click **Save**.

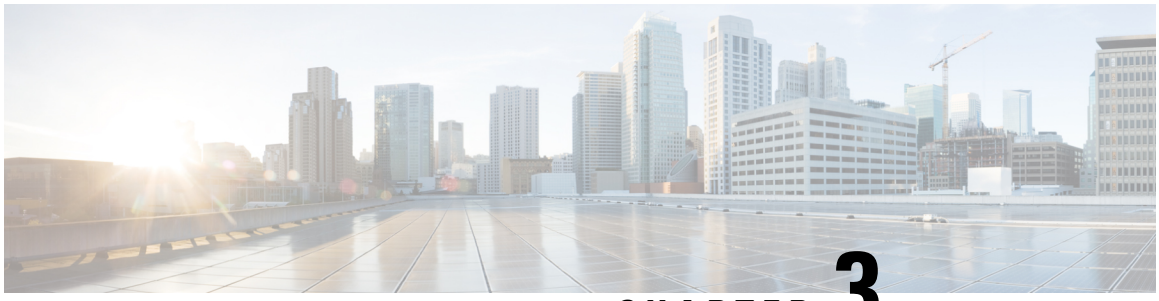
Set Up the Organization Tenancy

Procedure

Step 1 After *initial* log in as an admin, you are directed to a page that requires you to provide an organization name. Enter an organization name, then click **Next**.

Step 2 Set your personal profile preferences and click **Submit**.

Note If at some point you want to move your subscription to another organization, you must remove the subscription ID as documented in Transfer a Subscription to Another Organization.



CHAPTER 3

Get Started with Crosswork Cloud Network Insights

This workflow lists the high-level tasks to quickly start using Crosswork Cloud Network Insights.

• Get Started with Crosswork Cloud Network Insights, on page 7

Get Started with Crosswork Cloud Network Insights

Crosswork Cloud Network Insights does not require any hardware setup. You only need to have the following information to immediately start using Crosswork Cloud Network Insights:

- A list of ASNs and prefixes you want to monitor
- An idea of the types of BGP updates you want to be alerted for

Note See Import Peers if you are migrating peers from BGPmon.

Table 1: High-level Crosswork Cloud Network Insights Get Started Workflow

Step	Action	Procedure and Notes
1	Gather ASN and prefixes you want to monitor.	—

Get Started with Crosswork Cloud Network Insights

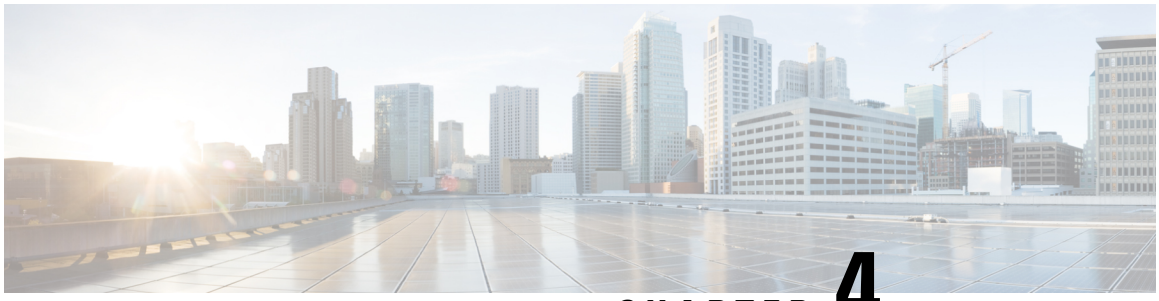
Step	Action	Procedure and Notes

2	Use **Express Setup** to quickly add ASN and prefixes to monitor. By default, Crosswork Cloud will create policies with the most common rules that can trigger alarms for BGP updates you want to be alerted for.
	The following policies and rules are created:
	• ASN policy
	  • Unexpected AS Prefix
	• Prefix policy
	  • AS Origin Violation
	  • Subprefix Advertisement
	  • Prefix Withdrawal
	  • ROA Failure
	  • ROA Expiry
		• Use External Routing Express Setup
		 > **Express Setup**

3	Fine tune your policies. Create policies to define what your BGP advertisements should look like and notify you when they don't. • Do you need to create more policies? What type of policies? • What type of rules should you add? • Do you have too many alarms? Do you need to change threshold values?	• Alarms—View active alarms triggered by the policies you just created. > **Monitor** > **Alarms** • Policies—Create and modify policies to only generate alarms for BGP updates you are interested in. > **Configure** > **Policies** • Notification Endpoints—Define how or where you want to receive alarm notifications. These can be defined during policy configuration or you can navigate to the following: > **Global** > **Notifications** • ASN Routing Reports—Create and receive daily reports (or generate one on demand) that highlight changes in route announcements and peering relationships for your Autonomous System. > **Configure** > **Reports**

Step	Action	Procedure and Notes
4	View and analyze BGP routing. • Who is receiving your ASN BGP advertisements? • What do the AS paths look like? Are they getting to the expected destinations? • Troubleshoot and help pinpoint events that might have led to an alarm. • Use APIs to perform configuration tasks such as subscribing to prefixes or ASNs, configuring notification endpoints, and specifying conditions under which an alarm is triggered. See API documentation (> **Documentation** > **APIs**) for more information.	• Prefix Looking Glass—Shows current peers, AS paths, and communities. > **Monitor** > **Prefixes** > ***prefix-ip-address*** > **Looking Glass** tab • ASN Looking Glass —Shows current prefixes and reporting peers. > **Monitor** > **ASNs** > ***asn-name*** > **Looking Glass** tab • Prefix Path Topology—Allows you to visualize all peer, transit, and origin ASN that are advertised in AS paths for a prefix at a selected time. The Path Topology tool also provides you insight to help troubleshoot issues that might have occurred with routing traffic for the prefix during a specified time. > **Tools** > **Path Topology** • Alarms—View active alarms when any condition in your policies are met. > **Monitor** > **Alarms** • BGP Updates—Displays the BGP advertisements and withdrawals that occurred during that time range. > **Monitor** > **BGP Updates**

Get Started with Crosswork Cloud Network Insights



CHAPTER 4

Get Started with Crosswork Cloud Traffic Analysis

This workflow lists the high-level tasks to quickly start using Crosswork Cloud Traffic Analysis.

Since Crosswork Cloud Traffic Analysis uses Crosswork Data Gateway for data collection, the workflow also includes high-level information on how to install and set up Crosswork Data Gateway.

• Get Started with Crosswork Cloud Traffic Analysis, on page 11

Get Started with Crosswork Cloud Traffic Analysis

Table 2: High-level Crosswork Cloud Traffic Analysis Set Up and Get Started Workflow

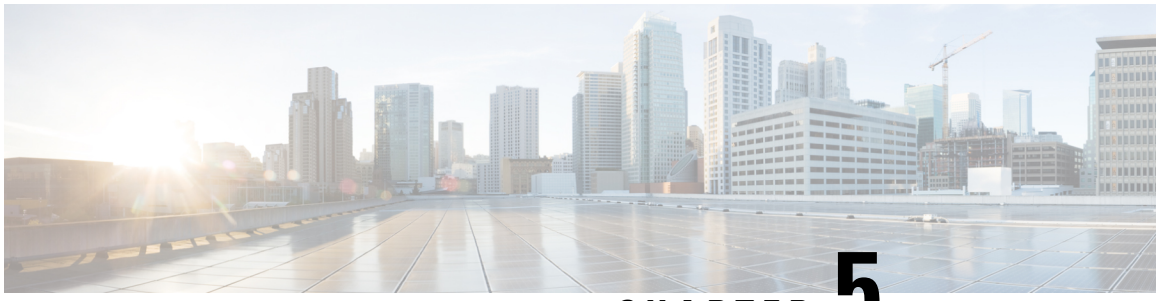
Step	Action	Crosswork Cloud Navigation and Notes
Crosswork Data Gateway Cisco Crosswork Data Gateway is initially deployed as a VM called Base VM that contains only enough software to enroll itself with Crosswork Cloud. Once the Crosswork Data Gateway is registered with Crosswork Cloud, Crosswork Cloud pushes the collection job configuration down to the Crosswork Data Gateway, enabling it to gather the data it needs from the network devices.		
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

Get Started with Crosswork Cloud Traffic Analysis

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 Data Gateway. • 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. Crosswork Data Gateway > **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 **Note** • For complete instructions on all supported platforms, see Install Crosswork Data Gateway. • As a quick reference, you can also see Install Crosswork Data Gateway Using vCenter vSphere Client, on page 23. This example takes you from getting the latest supported Crosswork Data Gateway image to verifying a successful installation.

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 Cisco 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	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 Trust Insights. > **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 **Note** To help confirm your environment is set up, you can also use the Crosswork Cloud Traffic Analysis Setup Checklist (> **Setup Checklist**)	Designate an External Interface > **Configure** > **Devices** > ***device_name*** > **Traffic Analysis** tab > **Interfaces**
10	View and create policies to define what normal traffic should look like and notify you when they don't.	Policies > **Configure** > **Policies**
What's Next? Setup is complete and you can begin using Crosswork Cloud Traffic Analysis.		

Step	Action	Crosswork Cloud Navigation and Notes
11	Start monitoring traffic and easily identify points of congestion and opportunities to provide better load balancing and optimization of your BGP traffic. • Do you see congestion? What changes could help with the congestion? • Can you split advertisements to move traffic flows from one peer to another? What is the impact of moving traffic between edge devices? • How do IP Routing tables relate to traffic flow in congested devices? • Where and who should you be peering with?	View traffic information: • View Device Traffic Details • View Interface Traffic Details • View ASN Traffic Details • View Prefix Traffic Details Tools you can use: • Optimize Interface Utilization—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. • Visually Compare Traffic—The tool compares traffic between like objects such as ASNs, prefixes, devices, and interfaces. • Traffic Drilldown—This tool allows you to easily view interface capacity and what traffic sources are contributing to it. • Peer Prospecting—This 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.



CHAPTER 5

Get Started with Crosswork Cloud Trust Insights

This workflow lists the high-level tasks to quickly start using Crosswork Cloud Trust Insights.

Since Crosswork Cloud Trust Insights uses Crosswork Data Gateway for data collection, the workflow also includes high-level information on how to install and set up Crosswork Data Gateway.

• Get Started with Crosswork Cloud Trust Insights, on page 15

Get Started with Crosswork Cloud Trust Insights

Table 3: High-level Crosswork Cloud Trust Insights Set Up and Get Started Workflow

Step	Action	Procedure and Notes
Crosswork Data Gateway Cisco Crosswork Data Gateway is initially deployed as a VM called Base VM that contains only enough software to enroll itself with Crosswork Cloud. Once the Crosswork Data Gateway is registered with Crosswork Cloud, Crosswork Cloud pushes the collection job configuration down to the Crosswork Data Gateway, enabling it to gather the data it needs from the network devices. The following steps are done outside of Crosswork Cloud.		
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

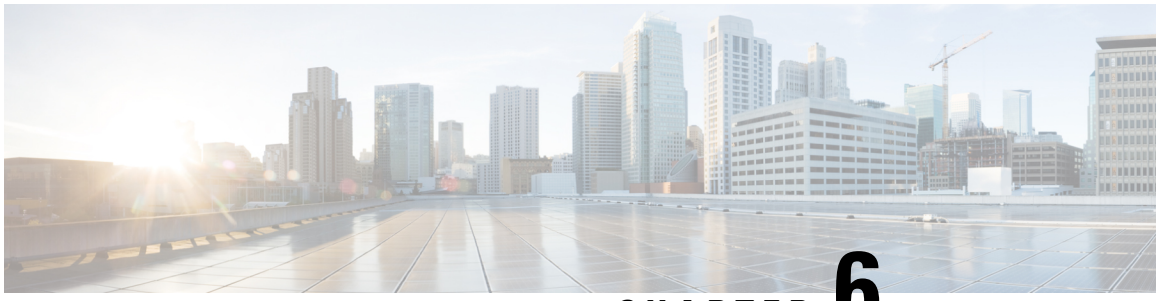
Get Started with Crosswork Cloud Trust Insights

Step	Action	Procedure 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 Data Gateway. • 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. Crosswork Data Gateway > **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 **Note** • For complete instructions on all supported platforms, see Install Crosswork Data Gateway. • As a quick reference, you can also see Install Crosswork Data Gateway Using vCenter vSphere Client, on page 23. This example takes you from getting the latest supported Crosswork Data Gateway image to verifying a successful installation.

Step	Action	Procedure and Notes
5	Authorize Crosswork Data Gateway access to Crosswork Cloud Trust Insights. **Note** Each Crosswork Data Gateway can be applied to one Cisco Crosswork Cloud 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	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**
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

Get Started with Crosswork Cloud Trust Insights

Step	Action	Procedure and Notes
11	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**
12	View and create policies to monitor device integrity.	Policies > **Configure** > **Policies**
What's Next?		
13	Verify software and view runtime signature analytics. • Does the software inventory reflect correct IOS XR inventory on a device? • Do software packages show verified software signatures (IMA "Observed Running") • Are software patches (SMU) successfully deployed across production systems? • Is software in compliance?	> **Monitor** >**Devices** > ***device-name*** **Trust Insights** tab
14	Verify hardware inventory.	View Device Inventory > **Monitor** > **Devices** > ***device-name*** **Trust Insights** tab. Click the **Inventory** tab.
15	View historical changes observed in systems. • Confirm a scheduled maintenance has been completed. • Further investigate known network issues • View device reboots or configuration changes • Is software in compliance?	View Device Changes > **Monitor** > **Devices** > ***device-name*** **Trust Insights** tab. Click the **Changes** tab.
16	Compare device configurations where a single device is chosen to be used as a baseline. Identify differences in installed software packages on similar devices deployed within production environments. Generate a "Punch List" of recommended changes to bring deviant devices into compliance.	Device Comparison > **Tools** > **Device Comparison**



CHAPTER 6

Troubleshoot Crosswork Cloud

- Troubleshoot Crosswork Data Gateway Connectivity, on page 19

Troubleshoot Crosswork Data Gateway Connectivity

The following steps will help you troubleshoot connectivity issues with your Crosswork Data Gateway and Crosswork Cloud.

Procedure

Step 1 In the main window, click **Data Gateways** and then click on the Crosswork Data Gateway for which you want to check connectivity.

Step 2 Ensure that the **Connectivity** field displays **Session Up**.

This indicates that the Crosswork Data Gateway is connected to the cloud.

Step 3 Ensure you have at least one device linked to the Crosswork Data Gateway.

Step 4 In the main window, click **Devices** and then click a device that is linked to the Crosswork Data Gateway.

Step 5 Click the **Status** tab.

Step 6 Ensure the Connectivity link between Crosswork Cloud and Crosswork Data Gateway is green, indicating the connection is working.

If the Connectivity link is red, which indicates there is an error, Crosswork Data Gateway is not connected to the cloud.

Step 7 Using SSH, log in to your Crosswork Data Gateway with the user name **dg-admin** and the password you specified when you installed Crosswork Data Gateway.

Step 8 Go to the Crosswork Data Gateway main menu, then select **Vitals > Controller Reachability** and verify that there is any established session. This will verify that the Crosswork Data Gateway can reach the default gateway and the DNS server.

If the Controller Reachability test failed, the failure is most likely due to one of the following issues:

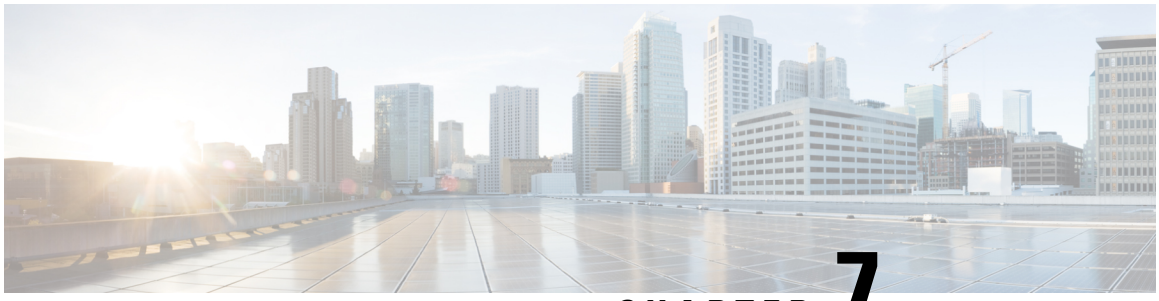
- Routing is not set up correctly to be able to get from the Crosswork Data Gateway to the internet.
- A firewall between Crosswork Cloud and Crosswork Data Gateway might be preventing communication. Ensure your firewall configuration allows cdg.crosswork.cisco.com and crosswork.cisco.com.

- A web proxy might be preventing communication. If you have a web proxy, you must have configured the required information during the Crosswork Data Gateway installation. Reinstall Crosswork Data Gateway and configure the web proxy to allow communication between Crosswork Cloud and Crosswork Data Gateway.

Step 9 From the Crosswork Data Gateway main menu, select **Docker Containers** and verify that one of the following images appear:

- cti-image for Crosswork Cloud Trust Insights
- cfi-image for Crosswork Cloud Traffic Analysis

This ensures the Crosswork Data Gateway was able to download the required image from Crosswork Cloud.



CHAPTER 7

Subscription Plans

- View Subscription Plan Options, on page 21
- Free Subscription Plan Requirement, on page 21

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

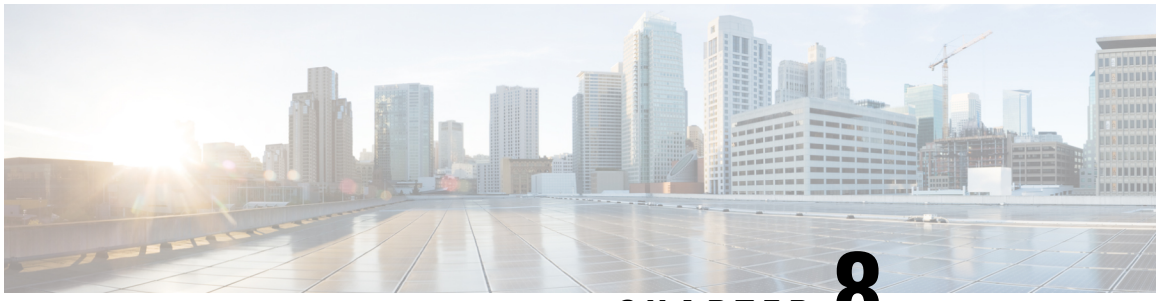
Free Subscription Plan Requirement

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 8

Supplemental Information

- Install Crosswork Data Gateway Using vCenter vSphere Client, on page 23

Install Crosswork Data Gateway Using vCenter vSphere Client

Crosswork Data Gateway is typically deployed within the same virtualization infrastructure that is used to deliver network management services. Detailed requirements are documented in the Installation Requirements section of the Cisco Crosswork Data Gateway Installation and Configuration Guide for Cloud Applications guide.

Confirm you also have the following information or requirements met prior to deployment:

	Requirement
☐	HTTPS/TLS Crosswork Data Gateway must be able to connect to external cloud services using HTTPS/TLS.
☐	Proxy, if required to access the internet
☐	Direct SSH access to routers Crosswork Data Gateway will connect to routers for data dossier collection using the SSH protocol. Any firewall policies designed to limit access between the management networks and routers may require adjustment to allow SSH access to routers from Crosswork Data Gateway. SSH collection is typically targeted at the IPv4 or IPv6 management ethernet address of routers, but any IP address on the router that allows inbound SSH access may be used.
☐	IP address of Management interface
☐	(Optional) IP address of southbound interface
☐	OVF Template information (see Step 3)

You can install Crosswork Data Gateway on various platforms (for example: VMware, OpenStack, and Amazon EC2). The following procedure is meant to be used as a quick reference to deploy the Crosswork Data Gateway VM using the vCenter vSphere Client. It provides *examples* of possible entries and assumes

you are familiar with VMware vCenter OVA installations. If you need further guidance or information on other platforms, see the following documentation:

- Cisco Crosswork Data Gateway Release Notes
- Cisco Crosswork Data Gateway Installation and Configuration Guide for Cloud Applications

Procedure

Step 1 Download the Crosswork Data Gateway image (*.ova) file and note the location where it is saved. If the file has a .dms extension, change it to .ova.

Step 2 Log in to vCenter vSphere Client, and then select **Actions > Deploy OVF Template**.

Step 3 Follow the Deploy OVF Template wizard prompts.

Table 4: Deploy OVF Template

Step	Description	Example
Select an OVF Template	Select the OVA image file you downloaded from the Cisco Software Download site.	**Local File > Choose File > Downloads > *cw-na-dg-4.5.0-19-release-20230119.uefi.ova***
Select a name and folder	Accept defaults, or enter an arbitrary name for this CCrosswork Data Gateway VM (default is taken from OVA file name) and select the datacenter where you want the VM to reside.	• Crosswork Data Gateway VM Name—***Crosswork Data Gateway 4.5*** • Datacenter—***ABCcompany_lab***
Select a compute resource	Within the datacenter, select the host (physical server) where the VM should be deployed.	***ABCcompany_hostserver1.com***
Review Details	VMware vCenter Server validates the OVA (may take a minute depending on network speed) then displays this screen with details for your review.	—
License Agreements	Review the license agreement.	—
Configuration	Select **Crosswork Cloud** as the deployment configuration. **Note** This is not always selected by default. Confirm that **Crosswork Cloud** is selected. If another option is selected, you will need to start the deployment from the beginning.	**Crosswork Cloud**
Select storage	Select the virtual disk and format. By default, the first virtual disk is selected. Ideally, select the disk that has the most free disk space. Confirm there are no errors under Compatibility.	• For production environment, choose **Thick Provision Lazy Zeroed**. • For development environment, choose **Thin Provision**.

Step	Description	Example
Select networks	Choose the appropriate destination network for each source network based on the number of vNICs you plan to use for sending traffic. I Start with vNIC0 and select a destination network that will be used. Leave unused vNICs set to the default value. • One vNIC—All traffic sent on vNIC0. • Two vNICs—Management traffic on vNIC0 and data traffic on vNIC1. • Three vNICs—Management traffic on vNIC0, northbound data traffic on vNIC1, and southbound data traffic on vNIC2.	In the following example, all traffic will be sent on vNIC0. vNIC1 and vNIC2 entries are ignored when only one active vNIC is selected later in the next **Customize template** step.

Step	Description	Example
Customize template	Configure IP addresses, vNIC role assignments, and so on.	The following options (at minimum) must be configured: • Host Information > Hostname—***Cisco-CDG*** • Host Information > Description—***TrustInsights-CDG*** • Host Information > Active vNICs • All passphrases **Note** These roles and passwords are used to log into Crosswork Data Gateway. • vNIC0 IPv4 or IPv6 address info. —***172.23.291.12*** If you chose more than 1 vNIC to be active (in last step) then fill the other vNICs (vNIC1 and vNIC2) details, otherwise skip the other vNIC sections. • DNS Servers > DNS Address—***171.70.168.183*** • DNS Servers > DNS Search Domain—***cisco.com*** • NTPv4 Servers >NTPv4Servers—***ntp.esl.cisco.com*** • Controller Settings > Crosswork Controller IP **Note** Enter **crosswork.cisco.com**. • Controller Settings > Crosswork Controller Port **Note** Enter **443**. • Proxy Server URL *if* you use a proxy or using a firewall. For more information, see Deployment Parameters and Scenarios.
Ready to complete	Review configuration summary.	—

Step 4 In the vCenter vSphere client **Recent Tasks** tab, view the status for the **Deploy OVF template** and **Import OVF package** jobs.

Step 5 When the deployment status is 100%, click the VM and select **Actions > Power > Power On**.

Step 6 After five minutes, verify that the installation was successful by accessing Crosswork Data Gateway via vCenter:

a) Right-click the VM and select **Open Console**

a) Enter username (**dg-admin** or **dg-oper** as per the role assigned to you) and the corresponding password (the one that you created during installation process) and press **Enter**.

Step 7 Verify that you can access Crosswork Data Gateway VM via SSH:

a) From your workstation terminal that has access to the Crosswork Data Gateway management IP, run the following command: ssh `<username>@<ManagementNetworkIP>`

where <*username*> is either **dg-admin** or **dg-oper** and <*ManagementNetworkIP*> is in an IPv4 or IPv6 format .

b) Enter the password (the passphrase information you entered in the OVF Template wizard).

© 2023 Cisco Systems, Inc. All rights reserved.