



# 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 1](#)







## Get Started with Crosswork Cloud Trust Insights

*Table 1: High-level Crosswork Cloud Trust Insights Set Up and Get Started Workflow*

Step	Action	Procedure and Notes
<p><b>Crosswork Data Gateway</b></p> <p>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.</p> <p>The following steps are done outside of Crosswork Cloud.</p>		
1	Confirm Crosswork Data Gateway requirements.	<a href="#">Installation Requirements</a>
2	Gather information needed during Crosswork Data Gateway installation. Make sure you have the following: <ul style="list-style-type: none"> <li>• A network where Crosswork Data Gateway can connect to Crosswork Cloud (Management Interface)</li> <li>• A network where Crosswork Data Gateway can connect to the devices (optional Southbound Interface)</li> <li>• IP address information for each interface</li> <li>• A proxy, if it is required to connect to the internet</li> </ul>	<a href="#">Deployment Parameters and Scenarios</a>

Step	Action	Procedure and Notes
3	<ul style="list-style-type: none"> <li>• 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.</li> <li>• For Crosswork Data Gateway versions earlier than 6.0.1, follow the steps described in <a href="#">Manually Add Crosswork Data Gateway Information</a>, then go to Step 6.</li> </ul>	<p><a href="#">Add Crosswork Data Gateway Information</a></p> <p>For Crosswork Data Gateway 6.0.1 or later:</p> <ol style="list-style-type: none"> <li>1. Crosswork Data Gateway &gt; <b>Data Gateways &gt; Use Enrollment Token</b></li> <li>2. Create or select an enrollment token.</li> <li>3. Copy the enrollment token somewhere so that it is readily available when you install Crosswork Data Gateway.</li> </ol> <p><b>Note</b> After you copy the enrollment token, you will need to install Crosswork Data Gateway before you can continue in Crosswork Cloud Traffic Analysis.</p>
4	<p>Install Crosswork Data Gateway.</p> <p>During Crosswork Data Gateway installation, you will need to paste the enrollment token in the following platforms:</p> <ul style="list-style-type: none"> <li>• VMware <ul style="list-style-type: none"> <li>• vCenter vSphere Client—Paste the token text into the <b>Auto Enrollment Package Transfer &gt; Enrollment Token UI</b> field</li> <li>• OVF Tool—Locate the script and under the ## Enrollment Token for Crosswork Cloud section, paste the token text after CloudEnrollmentToken=</li> </ul> </li> <li>• OpenStack—Locate the config.txt file and under the ## Enrollment Token for Crosswork Cloud section, paste the token text after CloudEnrollmentToken=</li> <li>• Amazon EC2—Paste the token in the CloudFormation template or as part of the user data after CloudEnrollmentToken=</li> </ul>	<p><a href="#">Install Crosswork Data Gateway</a></p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• For complete instructions on all supported platforms, see <a href="#">Install Crosswork Data Gateway</a>.</li> <li>• As a quick reference, you can also see <a href="#">Install Crosswork Data Gateway Using vCenter vSphere Client</a>. This example takes you from getting the latest supported Crosswork Data Gateway image to verifying a successful installation.</li> </ul>

Step	Action	Procedure and Notes
5	<p>Authorize Crosswork Data Gateway access to Crosswork Cloud Trust Insights.</p> <p><b>Note</b> Each Crosswork Data Gateway can be applied to one Cisco Crosswork Cloud application only. This means that you cannot use <i>this instance</i> of Crosswork Data Gateway for Crosswork Cloud Trust Insights.</p>	<ol style="list-style-type: none"> <li>1.  &gt; <b>Data Gateways &gt; Use Enrollment Token</b></li> <li>2. Click <b>Next</b>. The newly installed Crosswork Data Gateway should appear with then Enrollment State as <b>Pending</b>.</li> <li>3. Click <b>Allow</b> to authorize the Crosswork Data Gateway access.</li> </ol>
6	<p>Confirm you have all the Cisco IOS XR supported images, enrollment keys, certificates, and requirements needed for Crosswork Cloud Trust Insights.</p>	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS XR Supported Images</a></li> <li>• <a href="#">Verify Router Configuration</a></li> </ul>
7	<p>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.</p>	<p><a href="#">Configure Limited Privilege User</a></p>
8	<p>Add device credential profiles to be used when adding devices.</p>	<p><a href="#">Create Credentials</a></p> <p> &gt; <b>Configure &gt; Credentials &gt; Add Credential</b></p>
9	<p>Add devices.</p> <p><b>Note</b> If devices have already been added in Crosswork Cloud, you can simply link them to Crosswork Cloud Trust Insights ( &gt; <b>Data Gateways &gt; data-gateway-name &gt; Linked Trust Devices</b> tab).</p>	<ul style="list-style-type: none"> <li>• <a href="#">Add Devices</a></li> <li>•  <b>Devices &gt; Add Device</b></li> <li>• Confirm all connections are up. <b>Devices &gt; device_name &gt; Status</b> tab</li> </ul> <p><b>Note</b> You must have the following information populated:</p> <ul style="list-style-type: none"> <li>• Name</li> <li>• Hostname</li> <li>• Device timezone</li> <li>• Data Gateway</li> <li>• Credential group (defined in previous step)</li> </ul>
10	<p>Give it some time to collect data, then verify that the device data collection was successful.</p>	<p> &gt; <b>Monitor &gt; Devices &gt; device-name Trust Insights</b> tab</p>

Step	Action	Procedure and Notes
11	Initiate a dossier collection to get the latest device information	<a href="#">Collect Data for Trust Insights Device Dossier</a>  > <b>Configure &gt; Devices &gt; <i>device-name</i> &gt; Trust Insights &gt; Collect Dossier</b>
12	View and create policies to monitor device integrity.	<a href="#">Policies</a>  > <b>Configure &gt; Policies</b>
<b>What's Next?</b>		
13	Verify software and view runtime signature analytics. <ul style="list-style-type: none"> <li>• Does the software inventory reflect correct IOS XR inventory on a device?</li> <li>• Do software packages show verified software signatures (IMA “Observed Running”)</li> <li>• Are software patches (SMU) successfully deployed across production systems?</li> <li>• Is software in compliance?</li> </ul>	 > <b>Monitor &gt; Devices &gt; <i>device-name</i> Trust Insights tab</b>
14	Verify hardware inventory.	<a href="#">View Device Inventory</a>  > <b>Monitor &gt; Devices &gt; <i>device-name</i> Trust Insights tab.</b> Click the <b>Inventory</b> tab.
15	View historical changes observed in systems. <ul style="list-style-type: none"> <li>• Confirm a scheduled maintenance has been completed.</li> <li>• Further investigate known network issues</li> <li>• View device reboots or configuration changes</li> <li>• Is software in compliance?</li> </ul>	<a href="#">View Device Changes</a>  > <b>Monitor &gt; Devices &gt; <i>device-name</i> Trust Insights tab.</b> Click the <b>Changes</b> 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.	<a href="#">Device Comparison</a>  > <b>Tools &gt; Device Comparison</b>