

# Cisco Crosswork Network Controller 7.0 Release Notes

---

**First Published:** 2024-08-30

This document provides information about Cisco Crosswork Network Controller 7.0, including product overview, solution components, new features and functionality, compatibility information, and known issues and limitations.

## Overview

Cisco Crosswork Network Controller is a transport SDN controller that empowers customers to simplify and automate intent-based network service provisioning, health monitoring, and optimization in a multi-vendor network environment with a common GUI and API. Crosswork Network Controller simplifies operational workflows by consolidating both the service lifecycle and device management functions in a single integrated solution.

The solution offers intent-based network automation to deliver critical service orchestration and fulfillment capabilities, network optimization, path computation, service health monitoring, device deployment and management, and anomaly detection. Using telemetry gathering and automated responses, Cisco Crosswork Network Controller delivers network optimization capabilities that would be nearly impossible to replicate even with a highly skilled and dedicated staff operating the network.

The fully integrated solution combines core capabilities from multiple innovative, industry-leading products, including Cisco Network Services Orchestrator (NSO), Cisco Segment Routing Path Computation Element (SR-PCE), Crosswork Optimization Engine, and an evolving suite of applications operating on the Cisco Crosswork Infrastructure. Its unified user interface allows real-time visualization of the network topology and services and service and transport provisioning via a single pane of glass. Its feature-rich API allows operators to integrate the solution seamlessly with other applications they use to operate, monitor, and provision services on the network.

### Primary Use Cases:

- **Orchestrated service provisioning:** Provisioning of layer 2 VPN (L2VPN) and layer 3 VPN (L3VPN) services with underlay transport policies to define, meet, and maintain service objectives using the UI or APIs. Using Segment Routing Flexible Algorithm (Flex-Algo) provisioning and visualizing to customize and compute IGP shortest paths over a network according to specified constraints.

For this use case, Cisco Crosswork Advantage must be installed.

- **Real-time network and bandwidth optimization:** Intent-based closed-loop optimization, congestion mitigation, and dynamic bandwidth management based on Segment Routing and RSVP-TE. Optimization of bandwidth resource utilization by setting utilization thresholds on links and calculating tactical alternate paths when thresholds are exceeded.
- **Circuit Style Segment Routing Traffic Engineering (CS SR-TE) policy provisioning with network topology visualization:**
  - Straightforward verification of CS SR-TE policy configurations

- Visualization of CS SR-TE details, bi-directional active and candidate paths
- Operational status details
- Failover behavior monitoring for individual CS SR-TE policies
- A percentage of bandwidth reservation for each link in the network
- Manually triggered recalculations of existing CS SR-TE policy paths that may no longer be optimized due to network topology changes

For this use case, Cisco Crosswork Advantage must be installed.

- **Local congestion management:** Local Congestion Mitigation (LCM) provides localized mitigation recommendations within surrounding interfaces with the use of standard protocols. Data is gathered in real-time, and solutions are suggested when congestion is detected. LCM involves a “human-in-the-loop” approach, ensuring that the network operator has control over making changes. Additionally, LCM offers operators the choice to automate changes, enabling the system to implement changes to the network on its own. For this use case, Cisco Crosswork Advantage must be installed.
- **Visualization of network and service topology and inventory:** The topology UI, along with the various tables that can be accessed from it, allows you to easily assess the health of the network and drill down to see details about devices, links, and services.
- **Performance-based closed-loop automation:** Automated discovery and remediation of problems in the network by allowing Key Performance Indicator (KPI) customization and execution of pre-defined remediation tasks when a KPI threshold is breached. Health Insights and Change Automation functions must be installed for this use case.
- **Planning, scheduling, and automating network maintenance tasks:** Scheduling an appropriate maintenance window for a maintenance task after evaluating the potential impact of the task (using Crosswork Planning Design). Automating the execution of maintenance tasks (such as throughput checks, software upgrades, and SMU installs) using playbooks. For this use case, Health Insights and Change Automation functions must be installed.
- **Secured zero-touch onboarding and provisioning of devices:** Onboarding new IOS-XR devices and automatically provisioning Day0 configuration resulting in faster deployment of new hardware at lower operating costs. For this use case, Cisco Crosswork Essentials must be installed.
- **Visualization of native Segment Routing (SR) paths:** Using the traceroute SR-MPLS multipath command to get the actual paths between the source and the destination can be achieved using Path Query. A traceroute command runs on the source device for the destination TE-Router ID and assists in retrieving the paths. For this use case, Cisco Crosswork Advantage must be installed.
- **Provision, visualize, and analyze tree segment identifier policies in multipath networks:** Creating and visualizing static Tree-SID policies using the UI. Static mVPN Tree-SID policies, associated with existing or newly created L3VPN service models (SR MPLS point-to-multi-point), can be visualized and analyzed to manage and troubleshoot your multicast network efficiently. For this use case, Cisco Crosswork Advantage must be installed.
- **Transport slice provisioning:** Cisco Crosswork Network Controller offers direct support for network slicing at the OSI transport layer. Using this solution, network engineering experts can design slices around customer intents and add them to a catalog. Network line operators can assign the profile identified for a given customer to their endpoints and adjust the constraints according to the customer's requirements. Once the slice is provisioned, the path chosen can be visualized. Customers wishing for even greater

insight can use Service Health to gather additional performance data about the service. For this use case, Cisco Crosswork Advantage must be installed.

## Solution Components

Cisco Crosswork Network Controller components

**Table 1:**

Component	Version	Description
Platform Infrastructure	7.0	<p>A resilient and scalable platform on which all Cisco Crosswork components can be deployed. The infrastructure is based on a cluster architecture to ensure extensibility, scalability, and high availability.</p> <p>For installation, configuration, and administration procedures, refer to the following documents:</p> <ul style="list-style-type: none"> <li>• <a href="#">Cisco Crosswork Network Controller 7.0 Installation</a> guide.</li> <li>• <a href="#">Cisco Crosswork Network Controller 7.0 Administration</a> guide.</li> </ul>
Optimization Engine	7.0	<p>Provides closed-loop tracking of the network state and real-time network optimization in response to changes in the network state, allowing operators to effectively maximize network capacity utilization and increase service velocity.</p> <p>Provides traffic engineering visualization of SR-MPLS, SRv6, and RSVP-TE policies.</p> <p>For more information, see <a href="#">Cisco Crosswork Network Controller 7.0 Traffic Engineering and Optimization</a> guide.</p>
Service Health	7.0	<p>Overlays a service-level view of the environment and allows operators to monitor the health of services (for example, L2/L3 VPN) based on rules established by the operator.</p> <p>For more information, see <a href="#">Cisco Crosswork Network Controller 7.0 Service Health Monitoring</a> guide.</p>
Health Insights	7.0	<p>Performs real-time Key Performance Indicator (KPI) monitoring, alerting, and troubleshooting. It builds dynamic detection and analytics modules, allowing operators to monitor and alert network events based on user-defined logic.</p> <p>For more information, see <a href="#">Cisco Crosswork Network Controller 7.0 Closed-Loop Network Automation</a> guide.</p>

Component	Version	Description
Change Automation	7.0	Automates the process of deploying changes to the network.  For more information, see <a href="#">Cisco Crosswork Network Controller 7.0 Closed-Loop Network Automation</a> guide.
Data Gateway	7.0	A secure, common collection platform for gathering network data from multi-vendor devices that supports multiple data collection protocols, including MDT, SNMP, CLI, standards-based gNMI (dial-in), and syslog.  For more information, see <a href="#">Cisco Crosswork Network Controller 7.0 Administration</a> guide.
Element Management Functions	7.0	A library of functions that provides deep inventory collection, device management, alarm management, and software image management.  Zero Touch Provisioning with automatic onboarding of new IOS-XR and IOS-XE devices and provisioning of Day0 configuration, resulting in faster deployment of new hardware at a lower operating cost.  For more information, see <a href="#">Cisco Crosswork Network Controller 7.0 Device Lifecycle Management</a> guide.

Some of Cisco Crosswork Network Controller's functionality is enabled by the following products:

**Table 2:**

Products	Version	Description
Cisco Network Services Orchestrator	6.1.11.2	An orchestration platform that makes use of pluggable function packs to translate network-wide service intent into device-specific configuration. Cisco NSO provides flexible service orchestration and lifecycle management across physical network elements and cloud-based virtual network functions (VNFs), fulfilling the role of the Network Orchestrator (NFVO) within the ETSI architecture. It provides complete support for physical and virtual network elements, with a consistent operational model across both. It can orchestrate across multi-vendor environments and support multiple technology stacks, enabling extension of end-to-end automation to virtually any use case or device.  <b>Note</b> Function Packs are required to support compatibility with certain applications.

Products	Version	Description
Cisco Segment Routing Path Computation Element (SR-PCE)	24.2.1	An IOS-XR multi-domain stateful PCE supporting both segment routing (SR) and Resource Reservation Protocol (RSVP). Cisco SR-PCE builds on the native Path Computation Engine (PCE) abilities within IOS-XR devices, and provides the ability to collect topology and segment routing IDs through BGP-LS, calculate paths that adhere to service SLAs, and program them into the source router as an ordered list of segments.

## Cisco Crosswork Network Controller Packages

Cisco Crosswork Network Controller is distributed as two downloadable software packages (Essentials and Advantage) with an additional add-on package.

**Table 3: Cisco Crosswork Network Controller Software Packages**

Software Package	Supported Functionality
Cisco Crosswork Network Controller Essentials	<ul style="list-style-type: none"> <li>• Device Lifecycle Management (Inventory, ZTP, Fault, Performance, SWIM)</li> <li>• Physical Topology Visualization</li> </ul>
Cisco Crosswork Network Controller Advantage	<ul style="list-style-type: none"> <li>• Provisioning</li> <li>• Visualization</li> <li>• Service Health Monitoring</li> <li>• Path Compute</li> <li>• Traffic Engineering</li> <li>• Optimization</li> </ul>
Cisco Crosswork Network Controller Add-on <sup>1</sup>	<ul style="list-style-type: none"> <li>• Closed-Loop Automation</li> <li>• KPI Monitoring</li> </ul>

<sup>1</sup> Available only for users upgrading from prior Crosswork Network Controller releases.

## What's New

The following tables list the primary new features and functionality introduced in Cisco Crosswork Network Controller 7.0:

- [Table 4: Platform Infrastructure](#)
- [Table 5: Traffic Engineering](#)

- [Table 6: Topology](#)
- [Table 7: Change Automation](#)
- [Table 8: Service Health](#)
- [Table 9: Data Gateway](#)
- [Table 10: Device Lifecycle Management](#)
- [Table 11: Documentation](#)

**Table 4: Platform Infrastructure**

Feature	What's New?
AWS EC2 Support	<p>Support is available for deploying the following Cisco Crosswork Network Controller packages on the AWS EC2 platform.</p> <ul style="list-style-type: none"> <li>• Cisco Crosswork Network Controller Essentials package, excluding Zero Touch Provisioning</li> <li>• Cisco Crosswork Network Controller Advantage package, excluding Service Health</li> <li>• Cisco Crosswork Network Controller Add-on package: data export to 3rd party apps (CDG) &amp; geo redundancy (new)</li> </ul> <p>New capabilities supported for AWS EC2 platform:</p> <ul style="list-style-type: none"> <li>• Element management enhancements                             <ul style="list-style-type: none"> <li>• Software Image Management (SWIM) UI</li> <li>• Performance trends</li> <li>• Deeper inventory</li> <li>• Policy and service performance trend analysis</li> </ul> </li> <li>• FlexAlgo aware BWoD</li> <li>• Support for RON 3.0 Optics</li> </ul> <p>For information on deploying Crosswork Network Controller on AWS EC2, see <a href="#">Install Cisco Crosswork Network Controller on AWS EC2</a>.</p> <p>For information on the Crosswork Network Controller administrative tasks on AWS EC2, see <a href="#">Cisco Crosswork Network Controller 7.0 Administration Guide</a>.</p>

Feature	What's New?
Crosswork Network Controller deployed on a single VM	This release introduces support for deploying the Crosswork Network Controller solution on a single VM. The solution is deployed using a unified package that includes Crosswork Infrastructure, Embedded Collectors, and Element Management Functions, enabling you to leverage device lifecycle management functionalities. However, functionalities like service provisioning and overlay are only available on the cluster-based installation.
Geo redundancy	This release introduces the asynchronous data replication for geo redundancy clusters (on-premise L3 multi-site). It is no longer necessary to move the cluster into maintenance mode for data synchronization.
Dual stack support	Support for deploying Crosswork Network Controller with a dual stack (IPv4 and IPv6) configuration.
Installation enhancements	<ul style="list-style-type: none"> <li>The auto action feature has been added to automate application installation alongside cluster installation.</li> <li>Support for installing Cisco Crosswork Network Controller 7.0 on VMware vCenter and ESXi version 8.0.</li> </ul>
System access and security infrastructure	<ul style="list-style-type: none"> <li>Support for registering Crosswork components using the Crosswork Network Controller solution license.</li> <li>Support for launching the Single Sign On (SSO) service provider page from the Crosswork UI.</li> <li>Support for the automatic renewal of internal Crosswork certificates.</li> </ul>

Table 5: Traffic Engineering

Feature	What's New?
Bandwidth on Demand (BWoD) feature pack	You now have the option to have BWoD find a path with a specified <a href="#">Flexible Algorithm SID</a> . The acceptable SID values are 0, 1, and 128-255.
Alarms and Events	Traffic engineering alarms and events have been added or updated to be more consistent with other Crosswork services.
Virtual Routing and Forwarding (VRF)	Duplicate IP addresses on two interfaces in the same router are now supported when configured in a VRF table.
Interface Index (IfIndex)	Crosswork Network Controller now supports multiple IP addresses on a single IfIndex.
Links with both IS-IS Level 1 and Level 2 adjacencies	Crosswork Network Controller now discovers links with both ISIS Level 1 and Level 2 adjacencies. They are displayed on the topology map as dotted lines between devices.

Feature	What's New?
Cisco WAN Automation Engine (WAE) and Cisco Crosswork Planning plan file	<p>The plan file from Crosswork Network Controller now includes additional attributes: LSP MetricType, Dynamic, and applicable disjoint group information. A plan file is comprised of a series of tables that store information about a network, including topology, configuration information, traffic, failure state, and visual layout.</p> <p>For more information, see the <a href="#">Cisco Crosswork Solution Workflow Guide</a>.</p>
Interface Names	<p>When Element Management Functions (EMF) is installed, Crosswork Network Controller now abstracts any non-standardized interface name and populates the <code>interfaceName</code> value. As a result, only the <code>interfaceName</code> is used, which helps alleviate device telemetry, polling, and configuration problems.</p> <p>The <a href="#">Link Summary details</a> page displays the following field changes:</p> <ul style="list-style-type: none"> <li>• Interface Name—Displays the <code>interfaceName</code> value.</li> <li>• Interface Description—If applicable, displays any user specified text on the actual interface.</li> </ul>

**Table 6: Topology**

Feature	What's New?
Enhanced topology visualization of large (more than 50 endpoints) VPNs	<p>Enhanced navigation, provisioning, and visualization of the service overlay and details for large L3 VPNs containing up to 20,000 endpoints (UNI/PE-CE interface).</p> <p>When a user selects a VPN service in the UI that is too large to display in full (since a maximum of 50 endpoints can only be displayed once), they can click <b>Select endpoints</b> and choose from a list of endpoints to visualize the service overlay and details. The list shows only the endpoints on devices in the current selected device group. The list also includes filters to narrow down the list of endpoints, making it easier to select.</p> <p>Preconditions and limitations:</p> <ul style="list-style-type: none"> <li>• Visualization of large VPN support for L3VPN aligning with IETF L3 NM model.</li> <li>• Maximum number of vpn-node (PE) in the L3VPN: 4,000.</li> <li>• Maximum number of endpoints (UNI/PE-CE interface) in the L3VPN: 20,000.</li> <li>• Maximum number of policies or tunnels per large VPN: 5,000.</li> <li>• Maximum number of large VPN service instances in each deployment: 6.</li> <li>• Recommended provisioning of endpoints in a single request with a single L3VPN: 500.</li> </ul>



Feature	What's New?
Enhancements in the Topology UI - Links Visualization	A new <b>Links</b> tab displays all links on the map and a global links table in the <b>Devices</b> tab shows link details and metrics. Key metrics like bandwidth utilization, packet errors, packet drops, delay, and jitter are now shown in both the map and details panels, with delay and jitter available when Service Health is installed and SR-PM is enabled. You can also customize link color and metric thresholds in the Topology map and view historical data for collected metrics on the <b>Link Details</b> page.
Topology dashboard	A new <b>Topology</b> dashlet has been added to the <b>Dashboards</b> page, offering details on L2 and L3 links along with their associated metrics. When you click the L2 or L3 links in the dashboard, you will be directed to the Topology UI, where the corresponding map is displayed in the left pane. The <b>Devices</b> and <b>Links</b> tabs in the right pane offer detailed information about the devices and links on the map.

Table 7: Change Automation

Feature	What's New?
Support for check-sync action play	<p>A new stock play, <b>Perform Check Sync on the device</b>, is available to achieve check-sync. You can use this Play prior to running other operations in the Playbook or as part of pre-maintenance. This Play checks the device sync status with NSO and performs a sync-from (pulling the present device config into NSO) only when needed, based on the Playbook's sync parameter value. It reduces the Playbook execution time and ensures the NSO configuration matches the device configuration.</p> <ul style="list-style-type: none"> <li>• If the Playbook's sync parameter is set to True and the device is not in sync, it will sync the device with the NSO configuration, and the operation succeeds with an in-sync status.</li> <li>• If the sync parameter is set to False and the device is not in sync, the Playbook fails with a commit message.</li> <li>• If the device is already in sync, the operation succeeds.</li> </ul>

Table 8: Service Health

Feature	What's New?
Monitor Service Health using Cisco Provider Connectivity Assurance	<p>Crosswork Network Controller can leverage external probes from Cisco Provider Connectivity Assurance (formerly Accedian Skylight) to provide additional insights into the health of the L3 VPN services in the network.</p> <p><b>Note</b> Cisco Provider Connectivity Assurance integration is a limited-availability feature in this release. Contact your account team for more information. For more information, see the <i>Monitor Service Health</i> section in <a href="#">Cisco Crosswork Network Controller 7.0 Service Health Monitoring</a>.</p>

Feature	What's New?
L3 VPN service monitoring enhancements	Service Health supports large-scale VPN visualization by monitoring L3VPN services at the node level and creating an Assurance graph for each service at either the node or endpoint level. If the graph contains more than 50 endpoints, Service Health indicates that the graph is too large to view and prompts you to use the <b>Select Endpoints</b> option to select and view up to 50 endpoints.
Enhanced metrics and insights with SR-PM	When Segment Routing Performance Measurement (SR-PM) is enabled on your devices, Service Health collects and processes additional metrics like Delay, Delay Variance, and Liveness to assess the performance of links and the health of TE policies. It also offers historical data and trends for these metrics, providing valuable insights into network performance and trends.
Service Health dashboard	A new Service Health Dashboard displays a consolidated view of L2 VPN and L3 VPN services. If an SLA for a service is breached, the UI clearly indicates the break, making detection of problems easier.

**Table 9: Data Gateway**

Feature	What's New?
Support for dual-stack configurations	<p>Support for dual-stack configurations, enabling the system to establish connections using IPv4 and IPv6 protocols. This enables seamless, concurrent communication with various systems (such as NTP, DNS, and Syslog) and devices (SSH, SNMP, MDT) over IPv4 and IPv6. In dual-stack mode, IPv6 gets priority for all communication purposes.</p> <p>For information on configuring a dual stack when creating or editing a pool and adding destinations, see the <a href="#">Cisco Crosswork Network Controller 7.0 Administration Guide</a>.</p>
New custom package to support different file formats	<p>Support to flexibly manage the custom packages. This feature unifies the previously available upload structures by standardizing the structure for both system and custom packages. Also, Crosswork Network Controller now supports upload of multiple custom packages more efficiently.</p> <p>The enhanced Crosswork Network Controller UI enables uploading common package as well as the new aggregate package. The aggregate package facilitates the combination and merging of various file formats into a single, unified package.</p> <p>You can use the the aggregate custom packages for Embedded Collectors and Crosswork Data Gateway in a cluster deployment.</p> <p>For information on adding and downloading aggregate packages, see the <a href="#">Cisco Crosswork Network Controller 7.0 Administration Guide</a>.</p>

Feature	What's New?
Deployable on VMware vCenter version 8.0	<p>Support for installing Crosswork Data Gateway instances on VMware vCenter and ESXi version 8.0.</p> <p>For information on the installation of Crosswork Data Gateway on vCenter, see the <a href="#">Cisco Crosswork Network Controller 7.0 Installation Guide</a>.</p>
Embedded Collectors (Single VM)	<p>To simplify deployment, the Crosswork Network Controller can be set up on a single VM, though this comes with a trade-off in terms of scale and availability. This deployment model minimizes the reliance on external components by incorporating an embedded collector, replacing the need for external Crosswork Data Gateway VMs. In this model, the data gateway is installed as a lightweight CAPP within the single VM, reducing the need for separate data gateway nodes and significantly decreasing the deployment footprint. The data gateway functions as Embedded Collectors within the Kubernetes pods.</p> <p>For information on installing Embedded Collectors, see <a href="#">Cisco Crosswork Network Controller 7.0 Installation Guide</a>.</p>
A new Interactive Console menu option to modify the controller's IP or FQDN for data gateway enrollment and geo redundancy features	<p>The interactive menu now has a new option that enables you to modify the controller's IP or FQDN in these scenarios:</p> <ul style="list-style-type: none"> <li>• A data gateway may fail to enroll if deployed with an invalid controller IP.</li> <li>• A data gateway is registered, and the controller's VIP IP or IP is changed to an FQDN. This change might be necessary for Geo Redundancy configuration.</li> </ul> <p>For more information on changing the controller IP, see the <i>Configure Controller IP for Crosswork Data Gateway</i> section in the <a href="#">Cisco Crosswork Network Controller 7.0 Administration Guide</a>.</p>

**Table 10: Device Lifecycle Management**

Feature	What's New?
Device Management	<p>The following new features allow for customized monitoring and management of network devices.</p> <ul style="list-style-type: none"> <li>• Device tag creation and management. Tags can provide information such as the device's physical location and administrator's email ID, which can be used to group devices.</li> <li>• A comprehensive Network Inventory overview listing device names, types, hardware details, and operational statuses.</li> <li>• Manual inventory synchronization for up-to-date network device tracking.</li> <li>• Grouping of devices and ports which can be utilized for device management and performance monitoring data collection, based on specific parameters.</li> </ul>
Software Image Management (SWIM)	<p>Improved management of device software images, enabling seamless deployment, upgrades, and downgrades across a two-version range. Additionally, it supports specialized firmware upgrades for Field Programmable Devices (FPD) to maintain devices with unique firmware needs efficiently.</p>
Monitoring Policies	<p>Monitoring policies help you control how Crosswork Network Controller monitors your network. You can create and customize different monitoring policies to monitor network-wide device information and manage your network health. Monitoring policies are available for:</p> <ul style="list-style-type: none"> <li>• Device Health</li> <li>• Interface Health</li> <li>• LSP Traffic Policy</li> <li>• Optical SFP Interfaces</li> <li>• Optical ZR Pluggable Devices</li> </ul>
Alert Management	<p>Improved alert management for a more comprehensive system notification experience. Enhancements include:</p> <ul style="list-style-type: none"> <li>• Standardized alarms and events notifications integration and visibility.</li> <li>• Option to configure and customize your settings to receive alerts.</li> <li>• System-level event processing with throttling mechanisms to prevent system overload and maintain network stability and performance.</li> </ul>

Feature	What's New?
Zero Touch Provisioning	<ul style="list-style-type: none"> <li>• <b>ZTP integrated with EMF</b> ZTP is now integrated with Element Management Functions (EMF).</li> <li>• <b>UI/UX workflow changes</b> The ZTP sub-menu is integrated under the "Device Management" section of the UI main menu.</li> </ul> <p>For more information, see the <i>Zero Touch Provisioning</i> section in <a href="#">Cisco Crosswork Network Controller 7.0 Device Lifecycle Management</a>.</p>

Table 11: Documentation

Feature	What's New?
Documentation	<ul style="list-style-type: none"> <li>• An <a href="#">Information Portal</a> is now available for Crosswork Network Controller 7.0. The information is categorized by functional area, making it easy to find and access.</li> <li>• The <a href="#">Cisco Crosswork Network Controller 7.0 Device Lifecycle Management</a> details the steps for onboarding, managing, and monitoring network devices. It covers key aspects such as alarm management, monitoring policies, ZTP and software image management (SWIM).</li> </ul>

## Compatibility Information

The following tables list the hardware and software versions that have been tested and are known to be compatible with Cisco Crosswork Network Controller.

Many Crosswork Network Controller features depend on the underlying router XR/XE versions and the SR-PCE software. In the below tables, you can review those that are supported and working in combination with software versions on router platforms and SR-PCE.

- [Cisco Crosswork Infrastructure Support](#)
- [Device Management Support](#)
- [Cisco IOS Software Version Support](#)

## Cisco Crosswork Infrastructure Support

**Table 12: Cisco Crosswork Infrastructure Support**

Software	Supported Version(s)
Cisco Operating System <b>Note</b> This is an application-level compatibility.	<ul style="list-style-type: none"> <li>• Cisco IOS XR: 7.5.2, 7.6.1, 7.7.1, 7.8.1, 7.8.2, 7.9.1, 7.9.2, 7.10.1, 7.10.2, 7.11.1, 7.11.2, 24.1.x, 24.2.1, 24.2.11 (LNT)</li> <li>• Cisco IOS XE: 17.9.1, 17.12.1, 17.12.3</li> <li>• Cisco NX-OS: 9.2.1, 9.3.1, 10.2(3)</li> </ul>
Hypervisor and vCenter	<ul style="list-style-type: none"> <li>• VMware vCenter Server 8.0 (U2c or later) and ESXi 8.0 (U2b or later).</li> <li>• VMware vCenter Server 7.0 (U3p or later) and ESXi 7.0 (U3p or later).</li> </ul>
Browsers	<ul style="list-style-type: none"> <li>• Google Chrome—127 or later</li> <li>• Mozilla Firefox—128 or later</li> </ul>
Cisco Crosswork Data Gateway	<ul style="list-style-type: none"> <li>• 7.0</li> </ul>
Cisco Crosswork Network Services Orchestrator (Crosswork NSO)	<ul style="list-style-type: none"> <li>• 6.1.11.2</li> </ul> <p><b>Cisco Network Element Driver (NED)</b></p> <ul style="list-style-type: none"> <li>• Cisco IOS XR:               <ul style="list-style-type: none"> <li>• CLI: 7.52.2</li> <li>• NETCONF: 7.3.2, 7.4.2, 7.5.2, 7.6.2, 7.7.2, 7.8.2, 7.9.2, 7.10.2.1, 7.11.2, 24.2.1, 24.1.2</li> </ul> </li> <li>• Cisco IOS XE:               <ul style="list-style-type: none"> <li>• CLI: 6.106.9</li> </ul> </li> </ul> <p><b>Note</b> Additional function packs may be required based on the applications and features being used. See the <a href="#">Crosswork Network Controller 7.0 Installation Guide</a> for details.</p>
Cisco Segment Routing Path Computation Element (SR-PCE)	<ul style="list-style-type: none"> <li>• Cisco IOS XR 24.2.1</li> </ul>

## Device Management Support

Crosswork Network Controller is multivendor capable, leveraging open industry standard mechanisms and protocols such as BGP-LS, SNMP, gNMI, PCEP, segment routing, and NETCONF/YANG to communicate with network devices in a multivendor environment. See more details in the Crosswork Network Controller Solution Workflow Guide.

The following table details the Cisco device management support for IOS versions, SR-PCE, and Cisco devices.

We recommend that the SR-PCE version you use be equal to or higher than the PCC software version. PCC Cisco IOS XR 24.2.1 is recommended and has been validated to work with 7.0 features. Other listed PCC versions are supported, but may not support all features because of PCC version limitations.



**Note** For detailed information on supported devices for Element Management Functions, refer to [Crosswork Network Controller Supported Devices](#).

**Table 13: Device Management Support**

Cisco IOS XR	Cisco ASR 9901 (64-bit)	Cisco XRv 9000 <sup>2</sup>	Cisco 8000 series	Cisco NCS 5500/5700 series	Cisco NCS 540 series <sup>3</sup>	Cisco NCS 560 series	Cisco 8011 Series Fixed 1RU
7.5.2	✓	✓	✓	✓	✓	✓	✓
7.6.1	✓	✓	✗	✓	✓	✓	✓
7.7.1	✓	✓	✓	✓	✓	✓	✓
7.7.2	✓	✓	✓	✓	✓	✓	✓
7.8.1 + SMU (CSCwc93705)	✓	✓	✓	✓	✓	✓	✓
7.8.2	✓	✓	✓	✓	✓	✓	✓
7.9.1	✓	✓	✓	✓	✓	✓	✓
7.9.2	✓	✓	✓	✓	✓	✓	✓
7.10.1	✓	✓	✓	✓	✓	✓	✓
7.10.2	✓	✓	✓	✓	✓	✓	✓
7.11.1	✓	✓	✓	✓	✓	✓	✓
7.11.2	✓	✓	✓	✓	✓	✓	✓
24.1.x	✓	✓	✓	✓	✓	✓	✓
24.2.1	✓	✓	✓	✓	✓	✓	✓
24.2.11 (LNT)	✓	✓	✓	✓	✓	✓	✓

<sup>2</sup> The SR-PCE may be deployed on XRv9000 (VM or appliance).

<sup>3</sup> The SMU is available via the Cisco NCS 540-ACC-SYS Router or Cisco NCS 540x-ACC-SYS Router Software Download Center.

Cisco IOS XE Version	Cisco ASR 920	Cisco ASR 902 RSP 2	Cisco ASR 903 RSP 3	Cisco Catalyst 8000V Edge Software	Cisco ASR 1002-HX
17.9.1	✓	✓	✓	✓	✓
17.12.1	✓	✓	✓	✓	✓
17.12.3	✓	✓	✓	✓	✓



**Note** Segment Routing Traffic Matrix (SRTM) is only available in Cisco ASR 9000 devices.

### Cisco IOS Software Version Support



**Important** Element Management encompasses all the functionalities included in the Crosswork Network Controller Essentials package. For more detailed information, please refer to [Crosswork Network Controller Supported Devices](#).

Table 14: Cisco IOS Software Version Support

Operating System	Version	Service Lifecycle Management			Element Management <sup>4</sup>
		Service Provisioning	Traffic Engineering/Optimization	Monitoring/Assurance	
IOS-XR	7.5.2	✓	✓	✓	✓
	7.6.1	✓	✓	✓	✓
	7.7.1	✓	✓	✓	✓ <sup>5</sup>
	7.8.1	✓	✓	✓	✓ <sup>6</sup>
	7.8.2	✓	✓	✓	✓ <sup>7</sup>
	7.9.1 <sup>8</sup>	✓	✓	✓	✓ <sup>9</sup>
	7.9.2 <sup>10</sup>	✓	✓	✓	✓ <sup>11</sup>
	7.10.1	✓	✓	✓	✓



Operating System	Version	Service Lifecycle Management			Element Management <a href="#">4</a>
		Service Provisioning	Traffic Engineering/Optimization	Monitoring/Assurance	
	7.10.2	✓	✓	✓	✓
	7.11.1	✓	✓	✓	✓
	7.11.2	✓	✓	✓	✓
	24.1.x	✓	✓	✓	✓
	24.2.1	✓	✓	✓	✓
	24.2.11 (LNT)	✓	✓	✓	✓
IOS-XE <a href="#">12</a>	17.9.1	✓	✓	✓	✓
	17.12.1	✓	✓	✓	✓
	17.12.3	✓	✓	✓	✓

<sup>4</sup> Classic ZTP supports all IOS-XR versions found in the table.

<sup>5</sup> Secure ZTP is supported in 7.7.2.

<sup>6</sup> Only Secure ZTP config download is supported.

<sup>7</sup> Only Secure ZTP config download is supported.

<sup>8</sup> As SMUs become available, this document will be updated.

<sup>9</sup> Only Secure ZTP config download is supported.

<sup>10</sup> As SMUs become available, this document will be updated.

<sup>11</sup> Only Secure ZTP config download is supported.

<sup>12</sup> IOS-XE has limited support for advanced monitoring capabilities. NETCONF NED support is not available for IOS-XE.

## Scale Support

To support large-scale deployment, the components that make up Cisco Crosswork Network Controller are built with workload and endpoint load balancing using the Crosswork infrastructure's cluster architecture.

**Table 15: Scale Support**

Feature	Scale Support
Devices	15,000

Feature	Scale Support
Total Interfaces <sup>13</sup>	650,000 <sup>14</sup>
Provision of SR-TE policies and RSVP-TE tunnel (PCE-initiated)	100,000
IGP links	200,000
VPN Services (L2VPN, L3VPN)	150,000

<sup>13</sup> This is the total number of interfaces Cisco Crosswork can receive and process.

<sup>14</sup> This number has been validated with a total collection load of 390,000 interface entries across 15,000 devices (with 90,000 entries filtered out in the CDGs based on interface type). The number of CDG VMs can be increased to support higher collection loads.




---

**Note** Scale numbers will reduce if Layer 2 collection is enabled (for example, when LLDP, CDP, or LAG collection is enabled).

---




---

**Note** The Crosswork Network Controller Essentials package requires a minimum of 3 Virtual Machines (VMs) and the Crosswork Network Controller Advantage package requires a minimum of 5 VMs. For more information, see the [Crosswork Network Controller Installation Guide](#).

---

## Networking Technology Support for Traffic Engineering

The following is the networking support information for SR-PCE 24.2.1.

- [Supported Features](#)
- [Unsupported Features](#)

Table 16: Supported Features

Category	Description	Notes / Details
Segment Routing (SR)	SR-MPLS PCE initiated policies	Policies that are provisioned or discovered by Crosswork Network Controller.
	PCC initiated policies and ODN policies	Policies that are discovered by Crosswork Network Controller.
	Explicit path SR-TE policies	Policies that are PCC initiated (SID list with labeled SID list with addresses), PCE reported, PCE initiated. Includes SRv6 TE discovery of PCC initiated policies.
	Dynamic path SR-TE policies	PCC computed, PCE reported, PCE delegated
	Single consistent Segment Routing Global Block (SRGB) configured on routers throughout domain covered by Crosswork Network Controller	—
	Egress Peer Engineering (EPE) PeerAdjacency SIDs, PeerNode SIDs	<ul style="list-style-type: none"> <li>EPE must be configured on both ends of the eBGP link to appear in Crosswork Network Controller.</li> <li>EPE PeerAdjacency SIDs and PeerNode SIDs are represented as individual links in the Crosswork UI between the corresponding Autonomous Systems border routers (ASBR).</li> </ul> <p><b>Note</b> EPE PeerNode SIDs are identified by the Border Gateway Protocol Router ID (BGP RID) Loopbacks as the A and Z side link interfaces.</p> <ul style="list-style-type: none"> <li>Labels for both types of EPE SIDs, are shown as adjacency SIDs in the Crosswork Network Controller UI.</li> </ul>

Category	Description	Notes / Details
	Prefix SID	Regular/Strict Node SIDs + FA. Includes SRv6 Locators.
	Adjacency SID	B-flag (protected/unprotected), P-flag (Persistent). Includes SRv6 Locators.
	SR policy optimization objective min-metric (IGP, TE, and Latency)	PCE initiated provisioning and PCC initiated discovery
	SR policy path constraints (affinity and disjointness, protected segments)	<ul style="list-style-type: none"> <li>• Only 2 SR-MPLS policies per disjoint group or sub-id are supported. Disjoint Types: link, node, srlg, srlg-node.</li> <li>• Only 32-bit affinities supported. EAG (RFC 7308) is not reported by PCE and not visualized by Crosswork Network Controller.</li> </ul>
	Binding SID for explicit or dynamic policies	Discovered for PCC initiated and PCE initiated policies. It is configurable for PCE initiated policies.
	Profile ID (Discovered and configurable for PCE-init)	Parameter used for applying features on PCC to PCE initiated policies.
	Flexible Algorithm (Flex Algo) for SR-MPLS and SRv6 policies	<ul style="list-style-type: none"> <li>• Discover and visualize node Flex Algo participation.</li> <li>• Discover and visualize Flex Algo definitions.</li> <li>• SR policy IGP path respecting Flex Algo associated with prefix SIDs.</li> <li>• Displays pruned topology participating in FlexAlgo.</li> <li>• Preview and provision PCE initiated SRTE policies with a SID-Algo constraint.</li> </ul>
	Discovery and visualization of multiple candidate paths	—

Category	Description	Notes / Details
	Binding SIDs as Segment List Hops for SR policies	Discovery and visualization of PCC initiated policies.
	Tree-SID	Visualization and provisioning of PCE initiated policies.
	SR policies with Loopback IPs (Prefixes) other than TE router ID for headend/endpoint and prefix SIDs in segment list	Prefix (node) SIDs associated with specific IGP domain / area.
	Maximum SID Depth (MSD)	<ul style="list-style-type: none"> <li>• Per-node Base MPLS imposition MSD discovered via IGP/BGP-LS.</li> <li>• Per-node MSD discovered via PCEP session info.</li> <li>• Per-policy MSD.</li> </ul>
	Global Max Latency	Configured on PCE and applied to all PCE delegated SRTE policies with a latency metric.
	Inter-domain SRTE policies (inter-IGP domain, inter-AS)	PCE delegated and Bandwidth on Demand policies.
	Node SID reuse across different IGP domains	Recommended to not reuse node SIDs in adjacent IP domains. Inter domain explicit path policies with a label-only hop that is a node SID used in adjacent domains may be unresolvable if hop after ABR hop.
	Dynamic Circuit Style	Path computation and bandwidth reservation through the Circuit Style feature pack.
<b>SR-IGP</b>	Application-Specific Link Attribute (ASLA) Delay / TE metric	Crosswork collects and uses ASLA delay and TE metric in Flex Algo topology computations and SRTE policy IGP paths.
<b>SR-IGP</b>	Visualizing native SR-IGP path	Path Query OAM feature to use traceroute on device to report actual SR-IGP multi-paths to destination node ( <b>SR-MPLS only</b> )

Category	Description	Notes / Details
<b>RSVP</b>	PCE initiated tunnels (provisioned by or discovered by Crosswork Network Controller), PCC initiated tunnels discovered by Crosswork Network Controller	—
	ERO strict hops, ERO loose hops (PCC initiated only)	—
	FRR protection on Crosswork Network Controller provisioned tunnels	—
	Path optimization objective min-metric (IGP TE Latency)	—
	Path constraints (affinity, disjointness)	Only 2 RSVP tunnels per disjoint group or sub-id
	Binding Label (explicit   dynamic)	—
	Signaled Bandwidth	—
	Setup and Hold Priority	—
	Path Protection (partial support)	Paths discovered as independent tunnels if multiple paths are up. Cisco XR only reports active path. Other vendors may report all active paths.
<b>PCEP</b>	PCEP Session discovery	Each PCEP session a PCC has with a PCE along with its details is displayed as part of node details
<b>IPv4/IPv6</b>	Dual Stack IPv4 or IPv6	Nodes can be IPv4, IPv6 or IPv4/IPv6 capable
<b>IPv4</b>	Unnumbered Interfaces (partial)	Topology discovery, SR policies with unnumbered IF hops discovery/provisioning, LCM policy support
<b>IPv6</b>	IPv6 Link Local Interfaces	Discovery of IPv6 link local interfaces as part of topology and as a hop in an SRv6 TE policy
	IPv6 Router ID	Nodes with IPv6 and IPv6 Router ID only with support for SRv6 only

Table 17: Unsupported Features and Limitations

Category	Description	Notes / Details
Segment Routing (SR)	Provisioning multiple candidate paths for PCE-initiated SR policies via Crosswork Network Controller	—
	Per-Flow Policies (PFP)	PFP (ODN or manually configured) not supported in PCEP. This PFP is the mapping of forward class to PDP with matching color and EP.  Underlying PDP is reported as normal.
	Multiple segment lists per candidate path	This configuration is not supported in Crosswork.  These segment lists will not be discovered if configured on a PCC.  High level requirements: <ul style="list-style-type: none"> <li>• Discover multiple segment lists (with weights) per policy (TopoSvc, PCE, PCC)</li> <li>• Provision multiple segment lists (with weights) per policy (UI, PCED, PCE, PCC)</li> <li>• Visualize including showing IGP paths (UI, OE)</li> <li>• Compute paths of policies with multiple segment lists for LCM (OE, LCM)</li> </ul>
	Anycast SIDs	—
	SR policy provisioned (SR-PCE initiated) with IPv6 endpoints or hops	—
	SR-MPLS policy optimization objective min-metric with margin	Not supported for policies provisioned by Crosswork Network Controller. Margin is not discovered for PCC initiated policies.
	SR-MPLS policy constraints (resource exclusion or metric bound)	

Category	Description	Notes / Details
		Not supported for policies provisioned by Crosswork Network Controller. Constraints are not discovered for PCC initiated policies.
	Heterogeneous SRGBs	Different SRGBs configured on nodes are not supported. SRGB must be configured to ensure proper discovery and visualization of SR policy paths.
	Egress Peer Engineering (EPE) Peer Set SIDs	No discovery
	Routers that are not SR-capable	All nodes assumed SR capable when computing SR policy IGP paths. LCM and BWoD SR policy path computation will not exclude non-SR capable nodes in IGP path.
<b>SRv6</b>	PCE initiated provisioning of SRv6 policies is not supported.	—
	Traffic collection on SRv6 policies is not currently supported.	Requires telemetry (gNMI) for policy counters (no SNMP support)
<b>IGP</b>	ISIS Overload bit	Affects IGP paths for all policies and PCE path computation (BWoD, LCM). PCE reports but does not process.
	OSPF MADJ Interfaces	No support for discovering OSPF Multi-area adjacencies
	Multiple IGP instances on same interface	Single interface that participates in multiple IGP instances are not supported.



Category	Description	Notes / Details
<b>RSVP</b>	Configuring loose hop Explicit Route Object (ERO) in Crosswork	Only strict hops can be configured. If strict hops are not configured for every hop along the path and those hops are not remote interface IPs or loopbacks, unexpected behavior may occur
	Named tunnels configured on PCCs	Required for Juniper RSVP HEs
	Tunnels with Loopback IPs other than TE router ID for headend/endpoint and path hops	—
	Display of active FRR protected path in UI	Crosswork Network Controller will discover FRR tunnels which are displayed in UI but will not associate an actively protected tunnel with the FRR tunnel. Path in UI will not include FRR protected path when protection is active.
	P2MP tunnels	—
	Path protected RSVP LSPs	No association between paths discovered.
<b>LDP</b>	Local Congestion Mitigation (LCM) in Mixed SR/LDP networks	LCM will not work in a mixed SR/LDP network with PEs that are LDP only. LDP traffic destined to the LDP-only egress PE attempted to be steered into Autoroute LCM tactical policies will be blackholed
<b>IPv4</b>	IPv4 Unnumbered Interfaces	BWoD, Circuit Style Support, and RSVP
<b>IPv4/IPv6</b>	Secondary IP addresses for interfaces	Not supported. Unpredictable behavior if discovered.
<b>IPv4/IPv6</b>	Overlapping IP addresses in different IGP domains	IP addresses for IGP interfaces and nodes (router-ids) are assumed to be unique across all domains
<b>IPv6</b>	IPv6 Router ID	SR and RSVP not supported (SRv6 only)

## Important Notes

Take into consideration the following important information before starting to use Crosswork Network Controller 7.0:

- **Topology visualization:**

- Bandwidth utilization information is only available for physical interfaces and is not available for logical interfaces.

State	Link type	Interface	Utilization	In packet drops
Up	L3 OSPF L...	GigabitEthernet0/0/0/0	0% (565.8bps/1Gbps)	0%
Up	L3 ISIS IPv...	GigabitEthernet0/0/0/1	0% (1.68Kbps/1Gbps)	0%
Up	L2 Ethernet	TenGigE0/0/0/14	0% (28.01Kbps/10Gbps)	0%
Up	L3 ISIS IPv...	GigabitEthernet0/0/0/1.10	0%	0%

- **Crosswork Infrastructure:**

- It is recommended to deploy Crosswork Network Controller on a highly available cluster with shared storage.
- Managed devices, VM host, VMs, and all integrated components should use the same NTP source to avoid time synchronization issues.
- Confirm that the DNS and NTP servers are properly configured and reachable on the network the Crosswork Network Controller cluster will be using.
- Cisco recommends using Terminal Access-Control System Plus (TACACS+), Lightweight Directory Access Protocol (LDAP) or Role-Based Access Control (RBAC) to track access and prevent unauthorized usage of Crosswork Network Controller capabilities.
- During configuration, note the Crosswork Network Controller UI and CLI user names and passwords. Due to added security, the only way to recover the administrator password is to re-install the software.
- In situations where it is expected to work with SR-PCE (for L3 topology discovery), we recommend the use of dual SR-PCEs in an HA configuration.
- Use CSV files to quickly import and on-board device, credential, and provider information.

- **Obtaining geomaps for topology map renditions:**

To render geographical topology maps, if you do not have access to the map provider's website, you must download geo map files for the areas in the world you want displayed.

Crosswork Network Controller allows you to obtain downloadable geographical maps (geomaps) based on their specific topology mapping needs. If your environment allows contact with the map provider website we specify in Crosswork, you do not need to download the map files. If your environment does not allow outside access, you will need to download the map files for the areas where your network requires coverage.

- **Service provisioning:**

The Cisco Network Services Orchestrator sample function packs are provided as a starting point for service provisioning functionality in Crosswork Network Controller. While the samples can be used “as is” in some limited network configurations, they are intended to demonstrate the extensible design of Crosswork Network Controller. Answers to common questions can be found [here](#) and Cisco Customer Experience representatives can answer general questions about the samples. Support for customization of the samples for your specific use cases can be arranged through your Cisco account team.



**Note** For licensing and ordering information, work with your Cisco Partner or Cisco Sales representative to review the options described in the [Cisco Crosswork Network Controller Ordering Guide](#).

## Known Issues and Limitations

The table below shows known issues and limitations that should be taken into account before starting to work with Cisco Crosswork Network Controller 7.0.x.

- [Table 18: Infrastructure](#)
- [Table 19: Traffic Engineering](#)
- [Table 20: Service Health Monitoring](#)
- [Table 21: Service Provisioning](#)
- [Table 22: Data Gateway](#)
- [Table 23: Device Lifecycle Management](#)

**Table 18: Infrastructure**

Feature	Limitation
Fault and Alarm Synchronization	While geo redundancy enables a switch-over to an active cluster, it's important to take into account the timing of backups. Given the interval between the last backup and the restoration process, there is a loss of some alarm data from the devices. This is due to the time lag since the last backup was completed and restored.
Geo redundancy (with astack functionality)	If switchover is performed on a cluster on which Service Health is installed, the EOS data may contain partial metrics data (with intermittent gaps in the data metric sequence) for up to 24 hours.

**Table 19: Traffic Engineering**

Feature	Limitation
Transport Slice Provisioning	If the <b>Monitoring Status</b> for a Slice is enabled via API and the Slice is subsequently edited through the UI, the <b>Monitoring Status</b> is removed from the service and will need to be re-enabled if required.

Feature	Limitation
TE Dashboard	Traffic Utilization is not supported on Tree-SID and SRv6 policies.
	You cannot view the IGP path on the historical data when an event is selected.
	The metric type for BWoD policies is not visible on the TE Dashboard.
	Hop count metric and BWoD type are not shown in the TE Dashboard under metric/policy type.
	State and Path change events are not visible in the Historic tab of a policy until you zoom in by 5 to 6 clicks.
IPv4 Unnumbered Interfaces	Bandwidth on Demand and SR Circuit Style Manager feature packs will not factor in IPv4 unnumbered interfaces.
	Tree-SID policies are not supported.
	RSVP-TE PCE-initiated tunnels are not supported.
Tree-SID	Only static Tree-SID policies can be created via the UI. Also, you can only update and delete static Tree-SID policies that have been created via the UI.
	Tree-SID policies are only supported on devices running Cisco IOS XR software.
	PCE HA is not supported if the static Tree-SID policy was configured manually on the device (not via the UI).
	Tree-SID policies are not deleted from the UI when the SR-PCE in HA mode is down.
	IPv4 Unnumbered interfaces are not supported.
	Tree-SID policies are not supported in Label Switch Multicast (LSM) routing. In cases where LSM is enabled, IGP updates and traffic utilization data are not supported.
	LCM will not operate in portions of the network carrying Tree-SID LSPs.
	On Cisco 8000 Series Routers, only static Tree-SID policies with leaf role are supported.
	Tree-SID policy details do not show IPv6 router ID or SRv6 core information.

Feature	Limitation
SR-MPLS	In the SR-MPLS provisioning screen and while previewing an SR-MPLS policy with an IPv6 address, a parsing error is displayed instead of the correct error message: "Request Failed. Endpoint address is IPv6, IPv6 provisioning is not supported yet."
	Updating the SID constraint on an existing policy is not allowed by the SR-PCE. The modification screen gives a successful update message, instead of a warning message that it is not allowed.
APIs	The Topology API cannot discover and report IPv6 Link-Local style links.
	The Dashboard Export API cannot export CSV files to an external location. It can only export to /mnt/cw_glusterfs/bricks/rscoean/export.
BWoD	BWoD is disabled when the SR Policy Traffic field has 'Measured' selected and the Policy Violation field has 'Strict' selected.

Table 20: Service Health Monitoring

Feature	Limitation
Upgrade	<ol style="list-style-type: none"> <li>1. The <b>Monitoring Status</b> for existing services is displayed as <b>Unknown</b> by default.</li> <li>2. After the upgrade, some of the services (including the subservices <i>device.health subservice</i> and <i>sr.policy.pcc.pm</i>), may have the monitoring status as <b>Monitoring Error</b>. This is on account of some of the components being restarted (ASTACK, Crosswork Data Gateway tracker for example) during the upgrade.  To clear the error, stop and start the monitoring again for the service to clear the active symptom. However, if the monitoring error is on account of an issue with device health, then stop monitoring for all the services related to the device and start monitoring the services again to clear the error.</li> <li>3. Metric data is restored and available only after the Crosswork Data Gateway becomes active following an upgrade. There is no metrics data available for the duration that the Crosswork Data Gateway was inactive.  For example, if the Crosswork Data Gateway was active from October 10, 9:00 AM to October 10, 9:00 PM and was active again after an upgrade from October 11, 3:00 AM, an Event-of-Significance (EoS) generated on October 11 at 8:03 AM will lack metrics data between October 10, 9:00 PM and October 11, 3:00 AM.</li> </ol>

**Table 21: Service Provisioning**

Feature	Limitation
Large VPN Service	If you are creating a large VPN service using the Crosswork Network Controller UI and the service creation times-out and becomes stuck in-progress, Cisco recommends you delete the large VPN service using the Crosswork Network Controller UI or the NSO CLI. If the large VPN service is deleted using the NSO CFS UI, it will still be visible in the Crosswork Network Controller UI.
	Commit times for L3 VPNs with over 250 VPN nodes and 1,250 endpoints may take 10 minutes or more.
L2VPN service with RSVP-TE tunnel attached	<p>With an L2VPN service, the RSVP-TE can be attached by either <b>tunnel ID</b> (te-tunnel-id) or <b>tunnel service name</b> (ietf-te-service).</p> <p>If the RSVP-TE tunnel is attached by tunnel service name, when you navigate to <b>VPN Services &gt; Service details &gt; Summary</b> tab, the <b>Resources</b> section will display clickable links for additional RSVP-TE tunnel information.</p> <p>If the RSVP-TE tunnel is attached by tunnel ID, when you navigate to <b>VPN Services &gt; Service details &gt; Summary</b> tab, the <b>Resources</b> section will remain empty and no clickable links with additional RSVP-TE tunnel information will appear.</p>
VPN Service Provisioning	Service configuration data copied from Crosswork Network Controller VPN Services UI page cannot be used as a template for service provisioning from the Provisioning UI page. The Provisioning UI page has sample JSON/XML payload for each service type and should be used for service lifecycle management.

**Table 22: Data Gateway**

Feature	Limitation
Upgrade	When Crosswork Network Controller 6.0 is upgraded to 7.0, critical alarms remain uncleared, despite the data gateway VMs being <b>UP</b> and operational.

Table 23: Device Lifecycle Management

Feature	Limitation
Single VM Deployment	<p>When you change the device's Admin State from <b>UNMANAGED</b> to <b>DOWN</b>, the system automatically sets the state to <b>UP</b> because the auto-attach process attaches the device to the embedded collectors and modifies its Admin State from <b>DOWN</b> to <b>UP</b>.</p> <p>If changing the state to <b>DOWN</b> is necessary, you must manually change the state from the Edit Devices page as a next step.</p> <p>For information on editing the device information, see the <i>Edit Devices</i> section in <i>Cisco Crosswork Network Controller 7.0 Device Lifecycle Management</i>.</p>
Detailed Inventory	<p>The detailed inventory view in topology:</p> <ul style="list-style-type: none"> <li>• Slot, bay, and container are not shown in the Tree View.</li> <li>• If a node has only one leaf child node, then that node is shown as a merged entity with the child. This is observed for pluggable ports.</li> <li>• Only the entities with the Serial Number (SN) are shown in Detailed Inventory Tree View. The entity without a SN is hidden, and its child is attached to the parent of the hidden entity.</li> </ul> <p>Detailed inventory sync in topology view:</p> <ul style="list-style-type: none"> <li>• Optical ports for XR devices are merged with the corresponding SFP and the RSIP. The merging of ethernet ports for XR devices is currently not supported.</li> <li>• When clicking on the device node or the chassis node in the topology Tree View, both physical &amp; logical interfaces can be viewed. If you clicking on other nodes, only the physical interfaces can be viewed.</li> </ul>

Feature	Limitation
Alarms and Events	When an event is created for the first time, the <i>previous severity</i> for the event is set to <b>CLEARED</b> because there is no historical data. For subsequent occurrences of the same event, the <i>previous severity</i> is updated based on the last recorded severity of that event. This allows the system to track changes in event severity over time.
	In a cluster setup, you may encounter a call creation failure message for NATs, specifically for the <i>gnmi/fault-iosxr-alarm-manager</i> tagged alarm in IOS XR devices. This issue occurs when Kubernetes simultaneously creates multiple event processing instances. However, this error does not affect any other functionality.
	Alarm Severity is not updated on repeated events.  When an alarm is created in response to an incoming event, it initially reflects the event's severity (e.g., Major). However, if subsequent events of the same type continue to arrive with the same severity, the alarm severity is not updated and may reflect a previous state such as 'Cleared.' This behavior is intentional and designed to avoid unnecessary alarm updates.

## Product Documentation

An [Information Portal](#) is now available for Crosswork Network Controller 7.0. Information is categorized per functional area, making it easy to find and easy to access.

You can also access documentation for all Cisco Crosswork products at <https://www.cisco.com/c/en/us/support/cloud-systems-management/crosswork-network-automation/tsd-products-support-series-home.html>

The following documents are provided for Cisco Crosswork Network Controller 7.0.

**Table 24: Cisco Crosswork Network Controller 7.0 Documentation**

Document	What is Included
Cisco Crosswork Network Controller 7.0 Release Notes	The current document
<a href="#">Cisco Crosswork Network Controller 7.0 Installation Guide</a>	Shared installation guide for all the Cisco Crosswork applications and their common infrastructure. Covers: <ul style="list-style-type: none"> <li>• System requirements</li> <li>• Installation prerequisites</li> <li>• Installation instructions</li> <li>• Upgrade instructions</li> </ul>



Document	What is Included
<a href="#">Cisco Crosswork Network Controller 7.0 Administration Guide</a>	Shared administration guide for all the Cisco Crosswork applications and their common infrastructure. Covers: <ul style="list-style-type: none"> <li>• Managing clusters and data gateway</li> <li>• Data collection</li> <li>• High availability</li> <li>• Backup and restore</li> <li>• Onboard and manage devices</li> <li>• Set up maps</li> <li>• Managing users, access and security</li> <li>• Maintain system health</li> </ul>
<a href="#">Cisco Crosswork Network Controller 7.0 Solution Workflow Guide</a>	<ul style="list-style-type: none"> <li>• Solution overview</li> <li>• Supported use cases and their benefits.</li> <li>• Procedures for achieving the desired outcome for real-life usage scenarios using the Cisco Crosswork Network Controller UI.</li> </ul>
<a href="#">Cisco Crosswork Network Controller 7.0 Closed-Loop Network Automation</a>	Provides information on real-time Key Performance Indicator (KPI) monitoring, alerting, and troubleshooting. It also provides information on the automated process of deploying changes to the network.
<a href="#">Cisco Crosswork Network Controller 7.0 Service Health Monitoring</a>	Provides information on monitoring the health of L2VPN and L3VPN services. It provides insights into analyzing and troubleshooting degraded services, as well as visualizing service health status and logical dependency trees.
<a href="#">Cisco Crosswork Network Controller 7.0 Traffic Engineering and Optimization</a>	Provides information on how to visualize and configure traffic engineering in Crosswork Network Controller.
<a href="#">Cisco Crosswork Network Controller 7.0 Network Bandwidth Management</a>	Provides information on how to use Crosswork Network Controller feature packs. Feature packs are tools that tackle congestion mitigation and the management of SR-TE policies to find and maintain intent based bandwidth requirements.

Document	What is Included
<a href="#">Cisco Crosswork Network Controller 7.0 Device Lifecycle Management</a>	<ul style="list-style-type: none"> <li>• Device management</li> <li>• Software image management (SWIM)</li> <li>• Monitoring policies</li> <li>• Alert management</li> <li>• Zero touch provisioning</li> <li>• Supported devices</li> </ul>
<a href="#">Open Source Used in Cisco Crosswork Network Controller 7.0</a>	Lists of licenses and notices for open source software used in Cisco Crosswork Network Controller 7.0.x.
API Documentation	Advanced users can extend the Cisco Crosswork functionality using the APIs. API documentation is available on <a href="#">Cisco Devnet</a> .

#### Function Pack Documentation

- [Cisco NSO Transport SDN Function Pack Bundle 7.0.0 User Guide](#)
- [Cisco NSO Transport SDN Function Pack Bundle 7.0.0 Installation Guide](#)
- [Cisco Network Services Orchestrator DLM Service Pack 7.0.0 Installation Guide](#)
- [Cisco Crosswork NSO Telemetry Traffic Collector Function Pack 7.0.0 Installation Guide](#)
- [Cisco Crosswork Change Automation NSO Function Pack 7.0.0 Installation Guide](#)

## Bugs

If you encounter problems while working with Cisco Crosswork, check this [list of open bugs](#). Each bug ID in the list links to a more detailed description and workaround. You can use the Cisco Bug Search Tool to search for bugs.

1. Go to the [Cisco Bug Search Tool](#).
2. Enter your registered Cisco.com username and password, and click **Log In**.

The Bug Search page opens.




---

**Note** If you do not have a Cisco.com username and password, you can [register here](#).

---

3. To search for all Cisco Crosswork bugs, from the Product list select **Cloud and Systems Management > Routing and Switching Management > Cisco Crosswork Network Automation** and enter additional criteria (such as bug ID, problem description, a feature, or a product name) in the Search For field. Examples: "Optimization Engine" or "CSCwc62479"

4. When the search results are displayed, use the filter tools to narrow the results. You can filter the bugs by status, severity, and so on.



---

**Note** To export the results to a spreadsheet, click **Export Results to Excel**.

---

## Security

Cisco takes great strides to ensure that all our products conform to the latest industry recommendations. We firmly believe that security is an end-to-end commitment and are here to help secure your entire environment. Please work with your Cisco account team to review the security profile of your network.

For details on how we validate our products, see [Cisco Secure Products and Solutions](#) and [Cisco Security Advisories](#).

If you have questions or concerns regarding the security of any Cisco products, please open a case with the Cisco Customer Experience team and include details about the tool being used and any vulnerabilities it reports.

## Accessibility Features

For a list of accessibility features in Cisco Crosswork Network Controller, visit <https://www.cisco.com/c/en/us/about/accessibility/voluntary-product-accessibility-templates.html> (VPAT) website, or contact [accessibility@cisco.com](mailto:accessibility@cisco.com).

All product documents except for some images, graphics, and charts are accessible. If you would like to receive the product documentation in audio format, braille, or large print, contact [accessibility@cisco.com](mailto:accessibility@cisco.com).

## Support & Downloads

The Cisco Support and Downloads website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies.

Access to most tools on the Cisco Support and Downloads website requires a Cisco.com user ID and password.

For more information:

<https://www.cisco.com/c/en/us/support/index.html>

## Obtain Additional Information

Information about Cisco products, services, technologies, and networking solutions is available from various online sources.

- Sign up for Cisco email newsletters and other communications at:

<https://www.cisco.com/offer/subscribe>

- Visit the Cisco Customer Experience website for the latest technical, advanced, and remote services to increase the operational reliability of your network. Go to:

[https://www.cisco.com/c/m/en\\_us/customer-experience](https://www.cisco.com/c/m/en_us/customer-experience)

- Obtain general networking, training, and certification titles from Cisco Press publishers at:

<http://www.ciscopress.com>

