Cisco Crosswork Network Controller 5.0.x Release Notes

First Published: 2023-05-08

Last Modified: 2023-10-05

This document provides information about Cisco Crosswork Network Controller 5.0.x, including product overview, solution components, new features and functionality, compatibility information, and known issues and limitations.

Change History

The following table describes information that has been added or changed since the initial release of this document.

Date	Description
September 28, 2023	Cisco IOS XR Version 7.9.2 (SR-PCE and PCC) support has been added.

Overview

Cisco Crosswork Network Controller empowers customers to simplify and automate intent-based network service provisioning, monitoring and optimization in a multi-vendor network environment with a common GUI and API.

The solution combines intent-based network automation to deliver critical capabilities for service orchestration and fulfillment, network optimization, service path computation, device deployment and management, and anomaly detection with the option for automated remediation. 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), Cisco WAN Automation Engine (WAE), Cisco Crosswork Data Gateway, 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, as well as service and transport provisioning, via a single pane of glass. While its feature-rich API allows operators to seamlessly integrate the solution 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-level agreements (SLA), 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.

- **Real-time network and bandwidth optimization:** Intent-based closed-loop automation, 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.
- **Ability to provision Circuit Style Segment Routing Traffic Engineering (CS SR-TE) policies and visualize them in your network topology provides:**
  - 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
- **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 when congestion is detected, solutions are suggested. LCM has a “human-in-the-loop” aspect which ensures that the control of making changes in the network is in the hands of the operator.
- **Visualization of network and service topology and inventory:** Visibility into device and service inventory and visualization of devices, links, and transport or VPN services and their health status on maps with logical or geographical contexts.
- **Performance-based closed-loop automation:** Automated discovery and remediation of problems in the network by allowing Key Performance Indicator (KPI) customization and monitoring of pre-defined remediation tasks when a KPI threshold is breached. For this use case, Cisco Crosswork Health Insights and Cisco Crosswork Change Automation must be installed.
- **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 WAE Design). Automating the execution of maintenance tasks (such as throughput checks, software upgrades, SMU installs) using playbooks. For this use case, Cisco Crosswork Health Insights and Change Automation must be installed.
- **Secure zero-touch provisioning (ZTP) and onboarding 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 Zero Touch Provisioning must be installed.
- **Visualization of native SR paths:** Visualizing the native path using the traceroute SR-MPLS multipath command to get the actual paths between the source and the destination can be achieved using Path Query. With Cisco Crosswork Network Controller, a traceroute command runs on the source device for the destination TE-Router ID and assists in retrieving the paths.
- **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) using the Crosswork

Network Controller can be visualized and analyzed to assist in efficient management and troubleshooting of your multicast network.

Solution Components

Cisco Crosswork Network Controller components hosted on the Crosswork cluster:

Table 1:

Component	Version	Description
Cisco Crosswork Infrastructure	5.0	A resilient and scalable platform on which all of the Cisco Crosswork applications can be deployed. The infrastructure is based on a cluster architecture for extensibility, scalability, and high availability. For installation, configuration and administration procedures, refer the following documents: • Cisco Crosswork Network Controller 5.0 Installation Guide • Cisco Crosswork Network Controller 5.0 Administration Guide
Cisco Crosswork Data Gateway	5.0	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.
Cisco Crosswork Optimization Engine	5.0	Provides closed-loop tracking of the network state and real-time network optimization in response to changes in network state, allowing operators to effectively maximize network capacity utilization, as well as increase service velocity. Provides traffic engineering visualization of SR-MPLS, SRv6, and RSVP-TE policies.
Cisco Crosswork Health Insights (optional add-on)	5.0	A network health application that performs real-time Key Performance Indicator (KPI) monitoring, alerting, and troubleshooting. It builds dynamic detection and analytics modules that allow operators to monitor and alert on network events based on user-defined logic.
Cisco Crosswork Change Automation (optional add-on)	5.0	Automates the process of deploying changes to the network.

Component	Version	Description
Cisco Crosswork Active Topology	5.0	An application of Crosswork Network Controller that enables VPN (L2VPN, L3vVPN) service provisioning, service oriented transport (SR-MPLS, SRv6, CS-SR, RSVP-TE) provisioning and topology visualization of the provisioned services with the ability to customize the service provisioning and visualization through service model extensibility.
Cisco Service Health	5.0	An application that overlays a service level view of the environment and makes it easier for operators to monitor if services (for example, L2/L3 VPN) are healthy based on the rules established by the operator.
Cisco Crosswork Zero-Touch Provisioning (optional add-on)	5.0	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.

Products that integrate with Cisco Crosswork Network Controller:

Table 2:

Component	Version	Description
Cisco Network Services Orchestrator	6.1.0	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.
Cisco Segment Routing Path Computation Element (SR-PCE)	• 7.9.1 • 7.9.2	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.

Component	Version	Description
Cisco WAN Automation Engine (WAE)	7.6.1	A network design and planning tool used to visualize and optimize networks. The network abstraction contains all relevant information, including topology, configuration, and traffic details. Users leverage WAE to model, simulate and analyze failures, design changes, and the impact of traffic growth.

Cisco Crosswork Network Controller Packages

Cisco Crosswork Network Controller solution is distributed as two packages (Essentials and Advantage) and offers additional add-on services.

Table 3: Cisco Crosswork Network Controller Packages

Package	Contents	Description	Version
Cisco Crosswork Network Controller Essentials	Cisco Crosswork Optimization Engine	An application that provides closed-loop tracking of the network state and real-time network optimization in response to changes in network state, allowing operators to effectively maximize network capacity utilization, as well as increase service velocity.	5.0
	Cisco Crosswork Active Topology	An application of Crosswork Network Controller that enables VPN (L2VPN, L3vVPN) service provisioning, service oriented transport (SR-MPLS, SRv6, CS-SR, RSVP-TE) provisioning and topology visualization of the provisioned services with the ability to customize the service provisioning and visualization through service model extensibility.	5.0
	Cisco Element Management Functions (EMF) Services	A library of functions that provides deep inventory collection, alarm management and image management using Inventory, Fault, and Software Image Management (SWIM) functions.	5.0
Cisco Crosswork Network Controller Advantage	Cisco Crosswork Service Health	An application that overlays a service level view of the environment and makes it easier for operators to monitor if services (for example, L2/L3 VPN) are healthy based on the rules established by the operator. **Note** To install Service Health, you must first have the Crosswork Network Controller Essentials package.	5.0

Table 4: Cisco Crosswork Network Controller Add-On Services

Contents	Description	Version
Cisco Crosswork Change Automation	An application that automates the process of deploying changes to the network. Orchestration is defined via an embedded Ansible Playbook and then configuration changes are pushed to Cisco Network Services Orchestrator (NSO) to be deployed to the network.	5.0
Cisco Crosswork Health Insights	An application that performs real-time Key Performance Indicator (KPI) monitoring, alerting, and troubleshooting. Cisco Crosswork Health Insights enables programmable monitoring and analytics, and builds dynamic detection and analytics modules that allow operators to monitor and alert on network events based on user-defined logic.	5.0
Cisco Crosswork Zero Touch Provisioning	An application that streamlines on-boarding and provisioning of Day 0 configuration resulting in faster deployment IOS-XR and IOS-XE devices at a lower operating cost.	5.0

What's New

The table below lists the primary new features and functionality introduced in Cisco Crosswork Network Controller 5.0.x.

Table 5: New Features and Functionality in Cisco Crosswork Network Controller 5.0.x

Feature	What's New?
Circuit Style Segment Routing Traffic Engineering (CS SR-TE)	The CS SR-TE feature pack provides a bandwidth-aware Path Computation Element (PCE) to compute CS SR policy paths that you can visualize in your network. CS SR policies guarantee allocated bandwidth services with predictable latency and persistent bidirectional path protection of critical traffic. Unlike Bandwidth on Demand, where SR policies with requested bandwidth are created on a best effort basis, CS SR-TE reserves a percentage of bandwidth in the network and computes CS SR policy bidirectional failover paths with the requested bandwidth. CS SR-TE also maintains the accounting of all CS SR reserved bandwidth in the network. CS SR policies are typically used for high priority services, such as crucial monetary transactions or important live video feed, which require committed bandwidth with fast and fail-safe connections. Crosswork Network Controller enables you to provision CS SR-TE policy configurations and easily edit policies, as needed. In addition, the ability to visualize CS SR policies in your network topology allows you to easily verify CS SR policy configurations, details, and path states. With a few clicks you can view Active and Protective paths, operational status, reserved bandwidth pool size, and monitor path failover behavior for individual CS SR policies.
Tree Segment Identifier (Tree-SID) policy provisioning and L3VPN service model association	Tree-SID is used to implement multicast trees in segment routed transport networks. Using Crosswork Network Controller, the provisioning of static Tree-SID policies and the visualization of policies are rendered using the UI. Dynamic Tree-SID policies may be created directly on a device using an API. In addition, using Crosswork Network Controller, the ability to associate static Tree-SID policies with existing or newly created L3VPN service models is now available. • Static mVPN Tree-SID policies associated with existing, or newly created, L3VPN service models (SR MPLS point-to-multipoint) using the Crosswork Network Controller that can also be visualized and analyzed to assist in efficient management and troubleshooting of your multicast network. **Note** Dynamic Tree-SID policies can be visualized using the Traffic Engineering page. However, there will be no mapping on the Transport tab if it is attached to an L3 point-to-multipoint VPN service. • Configuring link affinities used to specify the link attributes that determine which links are suitable to form a path for the Tree-SID policy and maps each bit position or attribute with a color (making it easier to refer to specific link attributes). • Modifying existing static Tree-SID policies and mVPN Tree-SID policies associated with an L3VPN service model – both edit and delete – using the UI.

Feature	What's New?
Crosswork UI Improvements	

Feature	What's New?
	• Traffic Engineering Dashboard, which includes the TE Dashlet that provides: • A high-level summary of RSVP-TE tunnel, SR-MPLS, SRv6, and Tree-SID policy information (total policy count, policy state, metric types for all TE services, and specific data that is filtered upon a one-click selection). • Policies and Tunnels under traffic threshold for historical data by displaying RSVP-TE tunnels and SR-MPLS policies that have traffic below the defined threshold in the selected time period. This information may be used to find and filter the unused policies or tunnels. • Filtering the data on the dashlet based on the time range you want to view (date, 1 month, 1 week, 1 day, and 1 hour). • Policy and Tunnel Change Events: Displays all the policies and tunnels that have had a path or state change event ordered by the event count, within the selected time range. This information helps identify the unstable policies and tunnels. • Traffic Engineering event and historical data information associated with a device when viewing details for a policy or tunnel. For example, the traffic rate and event history for an SR-MPLS policy can be viewed by selecting the Historical Data tab and clicking on an event. By doing so, you can view the state of the policy or tunnel at that point in time and view additional details, such as Admin and Operational state, Segment type, accumulated metric, delegated PCE, and more so to drill down on the event details. • Enable/Disable Alarm Status Badge slider: The system allows you to enable or disable the Alarm Status Badge slider for devices and links across various topology views. Using the Alarm Status Badge, you can better focus the overlay on an area of interest when troubleshooting. • Configuration of the Traffic Engineering Data Dashboard Settings (and historical data) for the collection of policy and tunnel metrics, state and path changes, data retention intervals, and the utilization threshold for underutilized LSPs. • Global search in UI topology: You can now search within the Crosswork Network Controller topology map in the UI. This feature allows you to quickly locate devices based on the following criteria: • Civic Location (for example, San Jose) • Host/Device name (for example, NAT-01) • IP address (for example, 121.10.10.1.1) • Import and Export geographical objects using Keyhole Markup

Feature	What's New?
	Language (KML) format: • Using the Crosswork Network Controller UI, you can import and export KML files to exam, change, or add device geographical information and see the updates in the UI map. For example, you may use the export function to download your device's data in KML format to your system, exam and/or change the device details, and upload it into a map generator (such as Google Maps) to view your updated device information and coordinates outside of Crosswork Network Controller. You can then use the import function to upload the updated, or browse for a new, KML file back into Crosswork Network Controller. If changes were made, they will now appear in the geographical map after it refreshes. When using the import function, Crosswork Network Controller also provides a sample KML template. The sample KML template provides information on where to identify devices and their coordinates, an optional device name, and the IP address (IPv4 or IPv6) of a device with corresponding coordinates. This template can be used on your system before importing back into Crosswork Network Controller. • Traffic Engineering device details improvements that will provide options, after selecting a device from the topology map, to select different TE tabs (such as Links, Alarms, SR-MPLS, SRv6, RSVP-TE and others) that provide associated data for the selected device's policies and prefixes. **Note** For more information on Crosswork UI improvements, see the Crosswork Optimization Engine 5.0 User Guide section, *Visualize Traffic Engineering Services*.

Feature	What's New?
Crosswork Provisioning UI Improvements	• Dry Run for a deleted service: When decommissioning a service, only the configuration related to a service is deleted on the device. By implementing Dry Run, it shows the user the configuration that is deleted from multiple devices. • Edit in json configuration editor: Using the json configuration editor, you can highlight different details that make up the service configuration and edit them directly in the json editor before committing the configuration. • Clone existing services: Clone existing services and policies and utilize the json configuration editor to make changes to your cloned configuration. By cloning existing services and policies, you save time and ensure consistency across configurations. • **Show all fields** toggle option: When editing a service configuration, you can either hide multiple fields that do not pertain to the editable service configuration or you can view all fields by using the **Show all fields** toggle option. • Due to NSO Core Function Pack (CFP) model version upgrade, L2VPN, L3VPN or RSVP-TE upgrade is not supported from 4.x to 5.0. SR-TE upgrade from 4.x to 5.0 is supported. Direct upgrade from 3.x to 5.0 is not supported.
Security Framework	When adding a data destination, an additional security authentication layer is added to increase the security. In the **Administration** > **Data Gateway Global Settings** > **Data Destination** window, you can choose the authentication process type as: • Mutual-Auth: Authenticates external server and the CDG collector after the CA certificate, and Intermediate certificate or Key is uploaded to the Crosswork UI. • Server-Auth: Authenticates external server and the CDG collector after the CA certificate is uploaded to the Crosswork UI. • RADIUS: Support provided for user authentication with RADIUS (Remote Authentication Dial-In User Service) servers.

Feature	What's New?
Crosswork Infrastructure and Shared Services	• Support for offline licenses, solution-based licenses, and lab licenses • Support for user authentication via single sign-on (SSO) • Ability to log the user’s source IP address for auditing and accounting • High Availability support for Common Licensing Management Service (CLMS) • High Availability support for Element Management Functions (Inventory, Notification, Fault, and SWIM) • Support for visualization of device alarms and events • API and Notification support for alarms/events OSS integration • Ability to enable SMU configurations • Ability to configure timezone during installation of the Crosswork cluster
Services Overlay Visualization Enhancements	Ability to select Basic View or Extended View when visualizing a service overlay. The Basic View is a minimalistic view of your network services with no additional details, edge directions, router targets, or EVI/PW IDs. The Extended View includes all details, including edge directions, router targets, and EVI/PW IDs. The services overlay visualization enhancements apply to: • Point-to-Point Service Visualization • Any-to-Any Service Visualization (L2VPN and L3VPN) • Hub and Spoke Service Visualization (L2VPN and L3VPN) • Custom Service Visualization (L2VPN and L3VPN)

Feature	What's New?
Cisco Service Health	

Feature	What's New?
	• Service Health monitoring is available for both Basic Monitoring and Advanced Monitoring. **Note** In total, Basic + Advanced Monitoring provides up to 52,000 services that can be monitored. • Heuristic Package improvements include: • IPv6 support that enhances and extends the SRv6 feature support • New Basic and Advanced rules for L2VPN (E-LAN and E-Tree) for monitoring (including multipoint feature for E-LAN and E-Tree) • High Availability for all Service Health containers. • Assurance Graph improvements that include node aggregation and expand/collapse capabilities to view subservice summary information and associated subservices. • New subservices, such as: • Dynamic subservices implementation (also includes SR-ODN policy) • Reservation Protocol for Traffic Engineering (RSVP-TE) Tunnel • Bridge Domain • Mac Learning • Device badge feature displays an orange badge on a device in the topological view indicating there are down and/or degraded subservices underneath that should be identified and symptoms inspected. • Summary node feature summarizes the aggregated health status of child subservices and reports one consolidated health status to a service node. The Summary node feature is available in both L2VPN multipoint Basic and Advanced monitoring models. • Basic monitoring subservices: • Device – Summarizes the health status of all underlying Devices participating in the given L2VPN service. • Bridge Domain – Summarizes the L2VPN Service's Bridge Domain health status across all participating devices. • Advanced monitoring subservices (in addition to what is also available with Basic monitoring)

Feature	What's New?
	• EVPN – Summarizes the health status of all underlying subservices – BGP Neighbor Health & MacLearning Health across all participating PE endpoints and provides a consolidated overall EVPN health summary status. • Transport – Summarizes the health status of all underlying subservices – SR-ODN (dynamic), SR Policy (statically configured) and RSVP TE Tunnel, across all participating PE endpoints and provides a consolidated overall Transport health summary status. • SR-PCEP – Summarizes the health status of all the underlying subservices that are monitoring the PCEP sessions. Each underlying subservice monitors the PCEP session health on a particular device participating in the given VPN service. • Extended CLI support using new Service Health system device packages, that can derive exact sensor paths for metric health calculation, that can now be installed as a bundle when the Service Health application is deployed.
Documentation	• An Information Portal is now available for Crosswork Network Controller 5.0. Information is categorized per functional area, making it easy to find and easy to access. • The Cisco Crosswork Network Controller 5.0 Installation Guide covers installation of the cluster and installation of Crosswork applications on top of the infrastructure. This guide includes Cisco Crosswork Data Gateway installation. • The Cisco Crosswork Network Controller 5.0 Administration Guide covers setup and maintenance of the Crosswork system. There is no longer a Getting Started Guide for Cisco Crosswork Network Controller. This guide includes Cisco Crosswork Data Gateway and ZTP information. • The Cisco Crosswork Network Controller 5.0.x Solution Workflow Guide provides an overview of the solution and its supported use cases. It walks users step-by-step through various common usage scenarios to illustrate how users can work with the solution components to achieve the desired benefits.

Compatibility Information

Many features on Crosswork Network Controller depend on the underlying router XR/XE versions and the SR-PCE software versions to support it. Verify those are supported and working in the combination of software versions on router platforms and SR-PCE.

Table 6: Cisco IOS Software Version Support

Operating System	Version	PCE-Init	PCC-Init	NSO + CFP CLI	NSO + CFP NETCONF	Crosswork Infrastructure	Crosswork Optimization Engine	Crosswork ZTP (Secure)[1]	Service Health
IOS-XR	6.7.2	✓	✓	✓	✗	✓	✓	✗	✗
	7.0.2	✓	✓	✓	✗	✓	✓	✗	✓
	7.1.2	✓	✓	✓	✗	✓	✓	✗	✓
	7.2.1	✓	✓	✓	✗	✓	✓	✗	✓
	7.3.1	✓	✓	✓	✓	✓	✓	✓	✓
	7.3.2	✓	✓	✓	✓	✓	✓	✓	✓
	7.4.1	✓	✓	✓	✓	✓	✓	✓	✓
	7.4.2	✓	✓	✓	✓	✓	✓	✓	✓
	7.5.2	✓	✓	✓	✓	✓	✓	✓	✓
	7.6.1	✓	✓	✓	✓	✓	✓	✓	✓
	7.7.1[2]	✓	✓	✓	✓	✓	✓	✗	✓
	7.8.1	✓	✓	✓	✓	✓	✓	✓[3]	✓
	7.8.2	✓	✓	✓	✓	✓	✓	✓[4]	✓
	7.9.1[5]	✓	✓	✓	✓	✓	✓	✓[6]	✓
	7.9.2[7]	✓	✓	✓	✓	✓	✓	✓[8]	✓
IOS-XE	17.6.3	✓	✓	✓	✗	✓	✓	✓	✗
	17.7.1	✓	✓	✓	✗	✓	✓	✗	✗
	17.8.1	✓	✓	✓	✗	✓	✗	✗	✗
	17.9.1	✓	✓	✓	✗	✓	✓	✓	✓

[1] Classic ZTP supports all IOS-XR versions found in the table.

[2] Not supported on Cisco ASR 9000 (32-bit)

[3] Only Secure ZTP config download is supported.

[4] Only Secure ZTP config download is supported.

[5] As SMUs become available, this document will be updated.

[6] Only Secure ZTP config download is supported.

[7] As SMUs become available, this document will be updated.

[8] Only Secure ZTP config download is supported.

Note Currently, not all SR-PCE Cisco IOS-XR versions 7.9.1 and 7.9.2 and platform SMUs are available. As SMUs become available, this document will be updated.

Note Software Maintenance Updates (SMUs) are required for both PCC/Headend and SR-PCE versions indicated in the table. To download the Cisco IOS XR versions and updates, see the IOS XR Software Maintenance Updates (SMUs) document.

Note For more information on IOS/Platform support information for IOS-XR versions 6.7.2, 7.0.2, 7.4.2, 7.6.1 and IOS-XE version 17.6.3, see the Crosswork Optimization Engine 5.0 Release Notes.

The following table lists hardware and software versions that have been tested and are known to be compatible with Cisco Crosswork Infrastructure.

Table 7: Cisco Crosswork Infrastructure Support

Software	Supported Version
Cisco Operating System **Note** This is an application-level compatibility.	• Cisco IOS XR: 6.7.2, 7.0.2, 7.1.2, 7.2.1, 7.3.1, 7.3.2, 7.4.1, 7.4.2, 7.5.2, 7.6.1, 7.7.1, 7.8.1, 7.8.2, 7.9.1, 7.9.2 • Cisco IOS XE: 17.6.3, 17.7.1, 17.8.1, 17.9.1 • Cisco NX-OS: 9.2.1, 9.3.1, 10.2(3)
Hypervisor and vCenter	• VMware vSphere 6.7 or above. • VMware vCenter Server 7.0 and ESXi 7.0. • VMware vCenter Server 6.7 (Update 3g or later) and ESXi 6.7 (Update 1 or later).
Browsers	• Google Chrome—92 or later • Mozilla Firefox—70 or later
Cisco Crosswork Data Gateway	5.0

Software	Supported Version
Cisco Network Services Orchestrator (Cisco NSO)	• 6.1.0
	Cisco Network Element Driver (NED) • Cisco IOS XR: • CLI: 7.46.3 • NETCONF: 7.3.2, 7.315, 7.4.2, 7.5.2, 7.6.2, 7.7.2, 7.8, 7.9 • Cisco IOS: • CLI: 6.86.6 **Note** Additional function packs may be required based on the applications and features being used. See the Crosswork Network Controller 5.0 Installation Guide for details.
Cisco Segment Routing Path Computation Element (SR-PCE)	• Cisco IOS XR 7.9.1 • Cisco IOS XR 7.9.2

Scale Support

To support large scale deployment, the applications that make up Cisco Crosswork Network Controller (Cisco Crosswork Optimization, Cisco Crosswork Active Topology, and other applications) are built with workload and endpoint load balancing using the Cisco Crosswork infrastructure's cluster architecture.

The following scale support numbers only apply to Cisco Crosswork solution applications.

Table 8: Scale Support

Feature	Scale Support
Devices	25,000
Total Interfaces[9]	500,000[10]
Provision of SR-TE policies and RSVP-TE tunnel (PCE-initiated)	150,000
IGP links	200,000
VPN Services (L2VPN, L3VPN)	300,000

[9] This is the total number of interfaces that Cisco Crosswork can receive and process.

[10] This number has been validated with a total collection load of 650,000 interface entries across 25,000 devices (with 150,000 entries filtered out in the CDGs based on interface type). The number of CDG VMs can be increased to support higher collection loads.

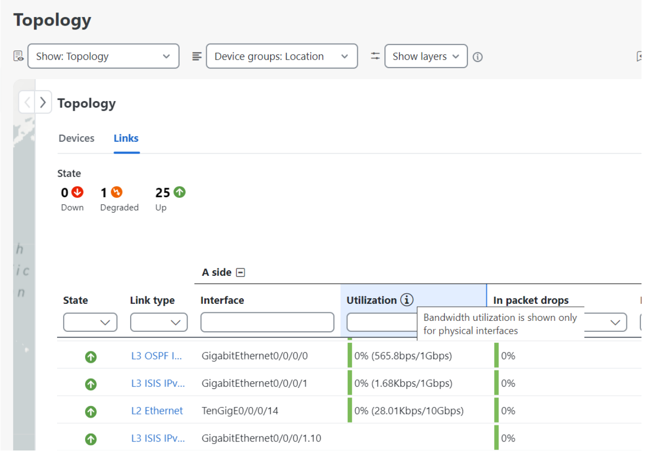
Note Scale numbers will reduce if Layer 2 collection is enabled (for example, when LLDP, CDP, or LAG collection is enabled).

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.

Important Notes

Take into consideration the following important information before starting to use Cisco Crosswork Network Controller 5.0.x:

- **Topology visualization:**
  - Bandwidth utilization information is only available for physical interfaces and is not available for logical interfaces.



State

0 Down · 1 Degraded · 25 Up

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

- **Cisco Crosswork Infrastructure:**
  - It is recommended to deploy Cisco Crosswork on a highly available cluster (vSphere HA) with shared storage.
  - Managed devices, VM host and the VMs 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 cluster will be using.
  - Use Terminal Access-Control System Plus (TACACS+), Lightweight Directory Access Protocol (LDAP) or Role-Based Access Control (RBAC) for auditing purposes.
  - During configuration, note the Cisco Crosswork 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.
  - Use CSV files to quickly import and on-board device, credential, and provider information.

- All unmanaged devices are counted towards the device limits associated with Crosswork licenses. To prevent this, delete your unmanaged devices in the Crosswork UI.
- **Obtaining Cisco Geomaps for topology map renditions:**

  Cisco Crosswork Network Controller allows users 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.
- **VPN Service Provisioning:**

  The Cisco NSO sample function packs are provided as a starting point for VPN service and RSVP-TE provisioning functionality in Cisco 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 Cisco Crosswork Network Controller. Answers to common questions can be found here and Cisco Customer Experience representatives can provide answers to 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 5.0.x.

Table 9: Known Issues and Limitations

Issue/Limitation	Context within Cisco Crosswork Network Controller
	Installation

Issue/Limitation	Context within Cisco Crosswork Network Controller
Crosswork cluster uses the following IP ranges for internal communications. This cannot be changed. As a result, these subnets cannot be used for devices or other purposes within your network. You are recommended to isolate your Crosswork cluster to ensure all the communications stay within the cluster. Please also ensure that address spaces do not overlap for any of the external integration points (e.g. connections to devices, connections to external servers that Crosswork is sending data to, connections to the NSO server, etc.). **Note** This is applicable for cluster installation and for adding a static route. IPv4: • 172.17.0.0/16: Docker Subnet (Infrastructure) • 169.254.0.0/16: Link local address block • 127.0.0.0/8: Loopback addresses • 192.88.99.0/24: Reserved, previously used for relay servers to do IPv6 over IPv4 • 240.0.0.0/4: Reserved for future use (previously class E block) • 224.0.0.0/4: MCAST-TEST-NET • 0.0.0.0/8: Current network, valid as source address only IPv6: • 2001:db8:1::/64: Docker Subnet (Infrastructure) • fdfb:85ef:26ff::/48: Pod Subnet (Infrastructure) • fd08:2eef:c2ee::/110: Service Subnet (Infrastructure) • fe80::/10: Link local • ::1/128: Loopback addresses • ff00::/8: IPv6 Multicast • 2002::/16: Reserved, previously used for relay servers to do IPv6 over IPv4 • 2001:0000::/32: Terredo tunnel and relay • 2001:20::/28: Used by ORCHID and not IPv6 routable	

Issue/Limitation	Context within Cisco Crosswork Network Controller
• 100::/64: Discard prefix, used in specific use-cases not applicable to Crosswork Zero Touch Provisioning • ::/128: Unspecified address, cannot be assigned to hosts • ::ffff:0:0/96: IPv4 mapped addresses • ::ffff:0:0:0/96: IPv4 translated addresses	

During the initial installation of Crosswork, the zookeeper instance may go into crashbackoff state continuously. At first, the UI health for one zookeeper pod will show down/degraded resulting in the zookeeper pod constantly restarting. The zookeeper_stdout.log logs for the pod will show the following (example of details): `[main] ERROR org.apache.zookeeper.server.quorum.QuorumPeer - Unable to load database on disk`. As a workaround, go to the node where the zookeeper pod is crashing and do the following:
`cd /mnt/cw_ddatafs/robot-zookeeper`
`rm -rf data/version-2`
`rm -rf log/version-2`
`kubectl delete pod robot-zookeeper-X --force --grace-period=0`
This removes the bad data and restarts the zookeeper pod so that it replicates from the two running instances.
	Installation

Issue/Limitation	Context within Cisco Crosswork Network Controller
• The number of nodes installed in Cisco Crosswork 5.0 must be equal or more than the number of nodes in earlier version of Cisco Crosswork. • Third-party device configuration in Device Management and Cisco NSO is not migrated and needs to be re-applied on the new version post migration. • Custom user roles (Read-Write/Read) created in earlier version of Cisco Crosswork are not migrated and need to be recreated manually on the new Cisco Crosswork version post migration. • Any user roles with administrative privileges in the earlier version of Cisco Crosswork must be assigned new permissions after the upgrade to continue being administrative users. • Crosswork Health Insights KPI alert history is not preserved as part of the migration. The system will need to be given some time to establish a new baseline for some KPIs. This may result in false alarms until the new base line is established. For more information, see the *Upgrade Cisco Crosswork* chapter in the Crosswork Network Controller 5.0 Installation Guide.	Upgrade

Issue/Limitation	Context within Cisco Crosswork Network Controller
• Sometimes, NETCONF reachability times out for IOS XE devices. To recover, try increasing the NETCONF reachability timer to a higher timeout value (for example, 120 seconds). • While retrieving device inventory via API from Cisco Crosswork, use page size of 200. • In case of Cisco NSO Layered Service Architecture (LSA), the migration of devices between Resource Facing Service (RFS) nodes is not supported. If you try to move the devices between RFS nodes, it creates a duplicate device entry in Cisco NSO. See the Onboard and Manage Devices chapter in Cisco Crosswork Network Controller 5.0 Administration Guide for details and instructions on removing duplicates. • Although the integration between Cisco NSO and Device Lifecycle Management (DLM) is automated, manual action is needed after a Cisco NSO recovery when the device admin status must go through DOWN/UP states. In this case, you must manually listen to NSO notifications that notify degradation within NSO and retry the action while NSO is up.	Device Management
• Each time the job list (located on the left side) is refreshed in the Collection Jobs window, the corresponding job details pane (located on the right side) must be manually refreshed. • A user session will not be terminated when you close the tab or the browser. The only way to remove a user session is to either log out from Crosswork or terminate the session from the User window (**Administration** > **User and Roles** > **Active Sessions**).	UI

Issue/Limitation	Context within Cisco Crosswork Network Controller
• Alarms, faults, errors, or any status indications for Cisco Crosswork Data Gateway will not be reflected on the VM node or its operational state. • Alerting service can become unresponsive during stress testing. Alerts related to Crosswork applications may not be generated during this time. If this happens, Cisco Crosswork will recover the alerting by automatically restarting the service. • If the node containing the Cisco Crosswork orchestrator is restarted, it might take up to 10 minutes before the health of the cluster can be viewed.	Alerts
• SR-PCE is required for L3 link topology mapping. • Enable traps on routers to receive L2 link down and up status changes quickly. Otherwise, it may take one SNMP poll cadence (default is 5 minutes) to see the L2 link status change. • If you have configured only GNMI-based collection and the bandwidth value on the interface is modified, the UI displays the original interface bandwidth rather than the updated or reduced bandwidth. However, the feature pack's (CSM, BWoD, LCM) back end computes the bandwidth using the revised value from SR-PCE for that interface.	Topology
Cisco Crosswork will not allow you to power off two hybrid nodes at the same time. If a system loses a hybrid node due to any faults, it must be replaced as soon as possible.	High Availability
If you restart microservices for a Crosswork application, the microservice may appear removed upon restart, but the application will continue to show a healthy status.	Crosswork Manager
• Fault service does not generate the SWT_SWITCH_DOWN alarm when a device becomes unreachable. • Localization of the *ospfIfStateChange*, *ospfIfConfigError*, *ospfIfAuthFailure*, *ospfIfRxBadPacket*, and *ospfTxRetransmit* alarms happens to loopback() from day 1.	Cisco Element Management Functions (EMF) Services

Issue/Limitation	Context within Cisco Crosswork Network Controller
In rare cases, after the successful registration, the License Authorization Status in the Smart Licensing page is not changed and will continue to display as being in EVALUATION mode. As a consequence, the evaluation timer will be started and incorrect messages will be displayed to the user. As a workaround, please de-register and register the product again.	Smart Licensing
After importing a new custom Heuristic Package, if you then select Editing Monitoring Settings for an existing service to switch between monitoring levels (Basic/Advanced), the request to edit the settings will fail. Instead, after importing a new custom Heuristic Package, you must next stop or start an existing service.	Service Health
L2VPN MPLS-EVPN over ODN-based policy monitoring is only supported for multi-point and not point-to-point. If, in this situation, point-to-point is selected, there will be no subservices for the associated ODN policies in Service Health Assurance Graph even though, on the device, the service is up (good health) and the ODN policies that are instantiated are up (good health).	Service Health L2VPN over ODN
If you shut down an SR Policy (L2VPN EVPN SR-TE service with fallback enable with Y1731 configured) at one endpoint, it results in packet loss and the Y1731 peer MEP check fails with symptoms flapping between up and peer-mep-failed and cross-check-missing in the device.	SR Policy
If service monitoring fails due to transient errors, such as HPM “nats time out”, stop and then restart service monitoring.	Service Health
Only enable one discovery protocol (CDP or LLDP) on an ethernet link when enabling protocols in the Layer 2 (L2) discovery settings. If you enable both CDP and LLDP on the same ethernet link and enable both protocols in the L2 discovery settings, it will result in duplicate links in the UI.	Layer 2 Discovery

Issue/Limitation	Context within Cisco Crosswork Network Controller
After monitoring fails in one of the worker nodes in a cluster, stopping and restarting the monitoring again does not resolve the issue and the service remains in error state while Assurance Graph remains unavailable. After the node is recovered and is again up (with all CAPPs and pods in a healthy state), the service remains in error state.	Service Health
• Explicit Circuit Style policy creation in Crosswork Network Controller through NSO CFP is not supported. • With NSO CFP, Circuit Style policies are only supported with L2VPN VPWS. • NSO CFP does not check existing Circuit Style/Segment Routing (SR) policies that have the same Headend/Tailend color combination.	Crosswork Network Controller/Circuit Style provisioning though NSO Core Function Pack (CFP)
With Circuit Style, IOS XE and IPv6 are not supported.	Circuit Style
NSO service pack implementation should support proper handling of zombies and ensure that the delete service-state-change notifications be sent when a zombies for the service are removed for a proper integration with Cisco Crosswork Network Controller UI. Without this support, deleting or redeploy of a service from Cisco Crosswork Network Controller UI may not work as expected.	NSO service pack implementation
Service Health’s corresponding VPN remains in a healthy state (it does not fail or move to a degraded state) after the user powers off Cisco Data Gateway (CDG) and the collection jobs become degraded as expected. In this scenario, a user onboards devices attached to a CDG with no spare on the pool. An L3VPN service is created and is enabled to monitor with Advanced/gold profile. Once the Service Health service shows a healthy state, CDG is powered off and collection jobs become degraded. Because Service Health is live monitoring, the user would expect the corresponding VPNs to also become degraded or fail and not remain in a healthy state.	Service Health

Issue/Limitation	Context within Cisco Crosswork Network Controller
Service Health subservices end up in initialization state or monitoring failed state after the following scenario: Load devices with JSON IETF, with one device being version 17.9.1 OS and the other device being version 17.6.3 OS, and then increase the timeout for both ASR920s. Create a L3VPN service with Loopback, enable a device to monitor service health, and then review the status for all subservices. In result, only interface health is supported and collection jobs scheduled. In addition, other subservices get scheduled but end up in initialization state or monitoring failed state.	Service Health
L2VPN cannot support the use of the SRv6TE or SRv6TE ODN (via route policy).	Route Policy
Secure ZTP image upgrade from 7.5.2 to 7.8.1, or 7.9.1 for IOS-XR NCS 55xx platforms, will fail due to a defect. This defect is resolved and fix is available on newer releases (7.9.2 and 7.10.1 IOS-XR version). Users cannot perform secure ZTP image install on versions 7.8.1 and 7.9.1, but can still perform the Day0 configuration upgrade operation without the image upgrade on the above IOS-XR versions.	Zero Touch Provisioning (ZTP)
Configuration upgrade fails with large files for IOS-XE ASR920 devices in 17.9.1 version.	Zero Touch Provisioning (ZTP)
• Associating an SR-TE policy with L2VPN-MPLS-EVPN is not supported. • SR-TE policies are not supported with the following: L2VPN-ETREE-hub-spoke, L2VPN-ELAN-p2mp, L2VPN-ELAN-any-any.	SR-TE Policy
Explicit path is not supported for SRv6 policy. However, when provisioning an SRv6 policy, if the candidate path is configured prior to enabling SRv6, the Explicit Path option is visible and can be committed with no warning and the explicit path configuration is ignored when SRv6 policy is pushed to the devices. If SRv6 is enabled first, before configuring the path, the Explicit Path option is not visible due to no SRv6 explicit path support.	Provisioning an SRv6 policy and configuring the Path

Issue/Limitation	Context within Cisco Crosswork Network Controller
SR-ODN policy is not created on Traffic Engineering (TE) and Transport tabs even though the device's policy has an operational UP status. This occurs if the router-id of any device is updated. In result, the topology must be rebuilt by re-importing the PCE and restarting the topo-svc service so that functionality works as expected.	SR-ODN Policy
L2VPN services may get stuck in an "in-progress" state after provisioning from the NSO UI. After loading different types of services from the NSO UI and cleaning them up, if you then reprovision those cleaned up services, those services will become stuck in an in-progress state. In this case, re-deploy the services stuck in-progress state so services regain a success state.	L2VPN Services
For the brownfield or greenfield customized service models that have schema with node type **instance-identifier** in the yang model, the **Edit In Json Editor** and **Clone** operation might not always work as expected.	Provisioning UI
Custom templates cannot be created using the UI, nor can their contents be visualized in the UI. Custom templates created offline can be applied to service models via UI and API. However, topology map overlays and service configuration views will not display custom template configuration.	Provisioning UI
Services can be provisioned to devices when devices are not mapped to Cisco Crosswork Network Controller or are operationally down, provided they are reachable and in sync with NSO.	Provisioning UI

Product Documentation

An Information Portal is now available for Crosswork Network Controller 5.0. Information is categorized per functional area, making it easy to find and easy to access.

The following documents are provided for Cisco Crosswork Network Controller 5.0.x.

Table 10: Cisco Crosswork Network Controller 5.0.x Documentation

Document	What is Included
Cisco Crosswork Network Controller 5.0.x Release Notes	This document

Document	What is Included
Cisco Crosswork Network Controller 5.0 Installation Guide	Shared installation guide for all the Cisco Crosswork applications and their common infrastructure. Covers: • System requirements • Installation prerequisites • Installation instructions • Upgrade instructions
Cisco Crosswork Network Controller 5.0 Administration Guide	Shared administration guide for all the Cisco Crosswork applications and their common infrastructure. Covers: • Managing clusters and data gateway • Data collection • High availability • Backup and restore • Onboard and manage devices • Zero touch provisioning • Set up maps • Managing users, access and security • Maintain system health
Cisco Crosswork Network Controller 5.0 Solution Workflow Guide	• Solution overview • Supported use cases and their benefits. • Procedures for achieving the desired outcome for real-life usage scenarios using the Cisco Crosswork Network Controller UI.
Open Source Used in Cisco Crosswork Network Controller 5.0	Lists of licenses and notices for open source software used in Cisco Crosswork Network Controller 5.0.x.
API Documentation	Advanced users can extend the Cisco Crosswork functionality using the APIs. API documentation is available on Cisco Devnet.

Related Product Documentation

This section provides links to documentation for products related to Cisco Crosswork Network Controller:

- Cisco Crosswork Optimization Engine 5.0:
  - User Guide

    - Release Notes

- Cisco Crosswork Change Automation and Health Insights 5.0:
    - User Guide
    - Release Notes
- Cisco Crosswork Data Gateway 5.0
    - Release Notes
    - Detailed information about Cisco Crosswork Data Gateway is available in the Cisco Crosswork Network Controller 5.0 Installation Guide and the Cisco Crosswork Network Controller 5.0 Administration Guide.
- Cisco Network Services Orchestrator 6.1.0
    - Documentation for Cisco NSO 6.1.0 can be downloaded here .
    - Additional information about Cisco NSO can be found here.
- Function packs:
    - Cisco NSO Transport SDN Function Pack Bundle 5.0.0 Installation Guide
    - Cisco NSO Transport SDN Function Pack Bundle 5.0.0 User Guide
    - Cisco Network Services Orchestrator DLM Service Pack 5.0.0 Installation Guide
    - Cisco Crosswork NSO Telemetry Traffic Collector Function Pack 5.0.0 Installation Guide
    - Cisco Crosswork Change Automation NSO Function Pack 5.0.0 Installation Guide
    - Open Source Used in Element Management Functions 5.0.0

You can 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

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.

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.

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

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

  http://www.ciscopress.com