

Cisco Crosswork Network Controller 7.0 What's New in this Release (EFT)

First Published: 2024-06-10

This document provides What's New in this Release information for Cisco Crosswork Network Controller 7.0 EFT.

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.

Solution Components

Cisco Crosswork Network Controller 7.0.x components hosted on the Crosswork cluster:

Table 1:

Component	Description
Cisco Crosswork Infrastructure	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.
Cisco Crosswork Data Gateway	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.

REVIEW DRAFT - CISCO CONFIDENTIAL

Component	Description
Cisco Crosswork Optimization Engine	<p>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.</p> <p>Provides traffic engineering visualization of SR-MPLS, SRv6, and RSVP-TE policies.</p>
Cisco Crosswork Health Insights (optional add-on)	A network health application that performs real-time Key Performance Indicator (KPI) monitoring, alerting, and troubleshooting. Using the UI and a robust set of APIs, operators can leverage any combination of Cisco-provided or their own custom-built KPIs to dynamically detect changes to the network's performance. When combined with Cisco Crosswork Change Automation remediation of issues detected in the network can be performed with a simple click or through predefined automated responses.
Cisco Crosswork Change Automation (optional add-on)	Automates deploying changes to the network to simplify day-to-day operations (implement normal changes) or to deploy changes manually or through automated responses to events detected using Crosswork Health Insights.
Cisco Crosswork Active Topology	An application of Crosswork Network Controller that enables VPN (L2VPN, L3VPN) service provisioning, service oriented transport (SR-MPLS, SRv6, CS-SR, RSVP-TE) provisioning and topology visualization. Through service extensibility features operators can customize both the service creation and service visualization capabilities provided by Crosswork Active Topology.
Cisco Service Health	An application that overlays a service level view of the environment, making it easier to monitor the health of L2VPN and L3VPN services. It enables you to see how issues impact services traversing the network. By providing visibility into the health of network services, it helps prioritize remediation efforts and informs operators about deviations from service level agreements (SLAs).
Cisco Crosswork Zero-Touch Provisioning (optional add-on)	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 7.0.x:

REVIEW DRAFT - CISCO CONFIDENTIAL**Table 2:**

Component	Description
Cisco Network Services Orchestrator	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)	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 WAN Automation Engine (WAE)	<p>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.</p> <p>Cisco WAE also provides traffic and topology analysis to Crosswork Change Automation and Crosswork Health Insights, playing a crucial role in various integrations, such as:</p> <ul style="list-style-type: none"> • Network Optimization: Provides traffic and topology analysis, helping optimize network resources and ensures efficient routing, capacity planning, and performance improvements. • Service Assurance: Integrates with service assurance platforms and monitors network health, detects anomalies, and triggers corrective actions. • SDN and NFV: Automates network provisioning and adapts to dynamic changes, ensuring service continuity and efficient resource utilization. • Multi-Vendor Environments: Supports multi-vendor networks and bridges gaps between different network elements, enhancing interoperability.

What's New in this Release

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

- [Table 3: Traffic Engineering](#)
- [Table 4: Service Health](#)
- [Table 5: Topology](#)
- [Table 6: Crosswork Data Gateway](#)
- [Table 7: Device Lifecycle Management](#)
- [Table 8: Platform Infrastructure](#)
- [Table 9: Documentation](#)

Table 3: 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 Flexible Algorithm SID. 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 now supports multiple IP addresses on a single IfIndex.
IS-IS Layer 1 and Layer 2	Crosswork now discovers L1 and L2 links. They are displayed on the topology map as dotted lines between devices.
Cisco WAN Automation Engine (WAE) plan file	You can now export a plan file from Crosswork to be used in WAE. 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.
Interface Names	<p>Crosswork 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 Link Summary details page now displays the following field changes:</p> <ul style="list-style-type: none"> • Interface Name—Reflects the <code>interfaceName</code> value. • Interface Description—If applicable, reflects the non-standardized interface name.

REVIEW DRAFT - CISCO CONFIDENTIAL**Table 4: Service Health**

Feature	What's New?
Monitor Service Health using Accedian Skylight	

DRAFT COPY

REVIEW DRAFT - CISCO CONFIDENTIAL

Feature	What's New?
	<p>Crosswork Network Controller can leverage external probing from Accedian Skylight to measure performance metrics of the L3VPN services. These metrics are then compared with the contracted SLA (defined in the Heuristic package), and the results are accessible on the UI for further analysis. You can monitor 2000 L3VPN services and 200 sessions per service.</p> <p>Note Monitoring L3VPN services using Accedian Skylight is only possible with Advanced monitoring and requires a Skylight Essentials license. See Skylight Licensing Tiers for more information. Sign up and create an account with the self sign-up tool to access the Skylight Solution documentation.</p> <p>Prerequisites</p> <ol style="list-style-type: none"> 1. Install the Accedian Skylight Solution. <p>Note This is a guided installation and will be led by Cisco's Customer Experience (CX) team.</p> <p>The Accedian Skylight Solution has the following components:</p> <ol style="list-style-type: none"> a. Skylight Analytics b. Skylight RoadRunner c. Skylight Orchestrator d. Agent - a SFP plugged into routers 2. Have the following certificates from Accedian Skylight downloaded on your local system or on a folder that can be accessed by Crosswork Network Controller: <ul style="list-style-type: none"> • CA certificate • Client certificate • Client key 3. Add Accedian Skylight as a Provider in Crosswork Network Controller <ol style="list-style-type: none"> a. Create a credential profile. <p>Navigate to Administration > Credential Profiles, click + to create a new profile. Enter a name. Enter protocols as HTTPS and gNMI. Add a username and password for both the protocols and click Save.</p> b. Create a certificate profile. <p>Navigate to Administration > Certificate Management, click + to add a certificate profile. Enter a name, select the Certificate Role as Accedian Provider Mutual Auth. Upload the</p>

REVIEW DRAFT - CISCO CONFIDENTIAL

Feature	What's New?
	<p>certificates (ca_cert.pem, client_cert.pem, and client_key.key).</p> <p>c. Onboard Accedian as a provider.</p> <p>Navigate to Administration > Manage Provider Access, click +. Enter details in the fields that are displayed and click Save.</p> <ul style="list-style-type: none"> • Provider Name: Enter a name for Accedian provider. • Credential profile: Select the credential profile that you had created for Accedian. • Family: Select ACCEDIAN_PROXY. • Certificate profile: Select the Accedian certificate profile that you created in Step 2. • Connection types: Supported protocols are automatically updated from the Accedian credential profile. • IP addresses: Enter IP addresses in IPv4 format • Ports: Enter 443 for HTTPS and a port value for GNMI. • Encoding Type: Select PROTO (Only encoding of type PROTO is supported). <p>d. Confirm reachability</p> <ol style="list-style-type: none"> 1. From the main menu, choose Administration > Manage Provider Access. 2. Confirm that the Accedian Skylight provider shows a green reachability status without any errors <p>High-Level Workflow</p> <p>After an L3VPN service is provisioned with the probe intent and service monitoring is enabled, a probe session to monitor the service starts automatically (by invoking RESTConf APIs).</p> <p>The probe intent and probe topology are learnt from provisioned service. The following probe intents are supported:</p> <ul style="list-style-type: none"> • Agent configurations: ne-id, VLAN, IP, sub-interface • Topology: point-to-point, hub-spoke, full-mesh <p>The list of RESTConf APIs that are invoked to provision probes sessions are:</p> <ul style="list-style-type: none"> • endpoint, session, service, session activation

REVIEW DRAFT - CISCO CONFIDENTIAL

Feature	What's New?
	<p>Service Health automatically subscribes to gNMI telemetry from the Accedian Skylight provider. Accedian Skylight streams the probe metrics to Crosswork Data Gateway. Crosswork Data Gateway collects the data using parameterized collection jobs. Service Health evaluates the metrics against the thresholds in the Heuristic Packages and reports symptoms and health status in the UI.</p> <p>View Probe Session Details on the UI</p> <p>You can view the probe session details for a service under the Probe Sessions tab on the Service Details page. Click the graph icon next to a probe session for a detailed view of the performance metrics.</p> <p>To view the Performance Metrics for a service in a carousel view, click the '...' icon in the Actions column.</p> <p>The Historical Data tab displays the historical data of the metric values for the last 24 hours or from the time when monitoring was enabled for the service, whichever is lesser.</p> <p>Reactivate Probe Sessions from UI</p> <p>You can reactivate the probe sessions for a L3VPN service with probe provisioning errors by clicking the Reactivate Probe for the service. The Probe Sessions page gets updated automatically to reflected the updated metrics if the probe session was reactivated successfully.</p>
Historical metric data in the Service Details page	<p>The Service Details page for L2VPN and L3VPN services includes historical data for selected metrics. The following metrics are displayed:</p> <ul style="list-style-type: none"> • L2VPN service - Latency, Jitter, Packet Loss (SD, DS), Delay (SR-PM), Variance (SR-PM) • L3VPN service - Delay, Variance <p>The historical data will be available for 90 days, with an option to select a specific time range to display a chart for each metric.</p>
Service Health dashboard	<p>A new Service Health Dashboard displays a consolidated view of L2VPN and L3VPN services. It also shows the Session and SLA Breaches of the L2VPN and L3VPN services.</p>

REVIEW DRAFT - CISCO CONFIDENTIAL**Table 5: Topology**

Feature	What's New?
Enhanced topology visualization of large VPNs	<p>Cisco Crosswork Network Controller 7.0 introduces enhanced navigation, provisioning and visualization of the service overlay and details for large VPNs that contain more than 50 endpoints and up to 5,000 VPN nodes.</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 at one time), they can click Select endpoints and choose from a list of endpoints so to visualize the service overlay and details. The list shows only the endpoints on devices in the current selected device group. The list also provides filters to easily narrow down the list of endpoints to select.</p> <p>Preconditions and limitations:</p> <ul style="list-style-type: none"> • Large VPN with more than 50 endpoints only supported for L3VPN with IETF NM model based service intent. • Maximum number of vpn-node (PE) in the L3VPN: 5,000. • Maximum number of endpoints (UNI/PE-CE interface) in the L3VPN: 20,000. • Maximum number of policies or tunnels per large VPN: 5,000. • Maximum number of large VPN service instances in each deployment: 6. • Recommended provisioning of endpoints in a single request with a single L3VPN: 500.
Enhancements in the Topology UI - Links Visualization	<p>The Topology UI has the following updates:</p> <ul style="list-style-type: none"> • The newly added Links tab shows all links in the displayed map on the left panel. • The Devices tab contains a global links table displaying all link details and metrics present in the topology map on the left panel. • The following link metrics are collected for Topology visualization in both map and details panels: <ul style="list-style-type: none"> • Bandwidth utilization, Packet error and Packet drops. • Delay and Jitter - These metrics are collected only when Crosswork Service Health is installed and SR-PM is enabled. • In the Topology map, you can display the link color based on a chosen metric, and define thresholds for these metrics from the Administration > Topology > Metric Thresholds page. • The Link Details page has a History tab to display historical data for all collected metrics.

REVIEW DRAFT - CISCO CONFIDENTIAL

Feature	What's New?
Topology dashboard	A new Topology dashlet has been added to the Dashboards page. It provides details about L2 and L3 links, along with link metrics. Clicking on L2 or L3 links in the dashboard takes you to the Topology UI, where the relevant map is displayed in the left pane. The Devices and Links tabs in the right pane provide details about the devices and links in the map.

Table 6: Crosswork Data Gateway

Feature	What's New?
Support for dual-stack configurations	<p>Crosswork Network Controller introduces support for dual-stack configurations, enabling the system to establish connections using both IPv4 and IPv6 protocols. With this enhancement, Crosswork can now seamlessly communicate with various systems (such as NTP, DNS, Syslog) and devices (SSH, SNMP, MDT) concurrently over both IPv4 and IPv6. In dual-stack mode, Crosswork gives priority to IPv6 for all communication purposes.</p> <p>For information on configuring a dual stack when creating or editing a pool and adding destinations, see <i>Cisco Crosswork Network Controller 7.0 Administration Guide</i>.</p>
A new custom package to support different file formats	<p>The Crosswork UI offers the capability to upload the aggregate package, a newly introduced custom package type. This innovative aggregate package feature allows you to combine and merge various southbound file formats into a single, unified package.</p> <p>For information on the adding and downloading the aggregate packages through the Crosswork UI, see <i>Cisco Crosswork Network Controller 7.0 Administration Guide</i>.</p>
Crosswork Data Gateway is deployable on VMware vCenter version 8.0	<p>Cisco Crosswork Network Controller 7.0 and Crosswork Data Gateway instances can be installed on VMware vCenter and ESXi version 8.0.</p> <p>For information on the installation of Crosswork Data Gateway on vCenter, see <i>Cisco Crosswork Network Controller 7.0 Installation Guide</i>.</p>
Embedded Collectors	<p>The Embedded Collectors is an on-premises solution that collects network data through collector services. The collectors support data collection from multivendors devices using secure protocols such as SNMP, CLI, gNMI, and Syslog. Later, the collector transfers the data to either Cisco Crosswork or external destinations, such as Kafka or external gRPC.</p> <p>For information on the installation of embedded collectors, see <i>Cisco Crosswork Network Controller 7.0 Installation Guide</i>.</p>

REVIEW DRAFT - CISCO CONFIDENTIAL

Feature	What's New?
Interactive menu option for changing the controller IP of a data gateway	<p>The interactive menu has been improved with a new option that enables you to modify the controller's IP or FQDN in these scenarios:</p> <ul style="list-style-type: none"> • A data gateway may fail to enroll with Crosswork Network Controller if deployed with an invalid controller. • A data gateway is registered with a Crosswork Network Controller, and the controller's VIP IP or IP is changed to an FQDN. This change might be necessary for Geo Redundancy configuration. <p>For more information on how to use the new menu option, see the <i>Configure Controller IP for Crosswork Data Gateway</i> section in <i>Cisco Crosswork Network Controller 7.0 Administration Guide</i>.</p>

Table 7: Device Lifecycle Management

Feature	What's New?
Device Management	<p>Network management has been enhanced with new features allowing for customized monitoring and management of network devices. These include:</p> <ul style="list-style-type: none"> • Tag Management window to manage the tags available for assignment to the devices in your network. Tags can provide information such as the device's physical location and its administrator's email ID, which can be used to group devices. • A comprehensive Network Inventory overview listing device names, types, hardware details, and operational statuses. • Device-level inventory control for precise management. • Regular inventory synchronization for up-to-date network device tracking. • Options for Device Groups and Port Groups are available, which can be utilized for performance monitoring data collection based on specific parameters.
Software Image Management	<p>Crosswork's Software Image Management (SWIM) now offers 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>

REVIEW DRAFT - CISCO CONFIDENTIAL

Feature	What's New?
Monitoring Policies	<p>Monitoring policies help you control how Crosswork monitors your network. You can create and customize different monitoring policies to monitor network wide device information to manage your network health. Monitoring policies are available for:</p> <ul style="list-style-type: none"> • Device Health • Interface Health • Optical SFP Interfaces • Optical ZR Pluggable Devices
Managing Alerts	<p>Crosswork's alert management has been improved to offer a more comprehensive system notification experience, incorporating alarms for immediate issues and events for significant occurrences. Enhancements include:</p> <ul style="list-style-type: none"> • Standardized alarms and events notifications for better integration and visibility. • Customizable metrics selection for detailed transport path views and historical trends. • Option to configure and customize your settings to receive alerts. • A unified view of service metrics along the transport path, depending on activated monitoring policies. • System-level event processing with throttling mechanisms to prevent system overload and maintain network stability and performance.
Zero Touch Provisioning	<ul style="list-style-type: none"> • UI/UX workflow changes <p>Zero Touch Provisioning sub-menu is integrated under "Device Management" section of the UI main menu, consolidating various individual sub-menus. This allows user to go to a landing page where Serial numbers/OVs, Config Files, ZTP Profiles and Devices can be configured while optimizing redundant functions and ensuring no impact to end-to-end ZTP operations.</p> <ul style="list-style-type: none"> • ZTP-SWIM integration for Image CRUD <p>ZTP and SWIM will be packaged together as part of Single VM based Crosswork Network Controller deployment.</p> <ul style="list-style-type: none"> • Enhance API-UI to support new vendor field <p>New Vendor field has been added in "Add device" "Add Configuration Files" and " Add Profile" menus.</p>

REVIEW DRAFT - CISCO CONFIDENTIAL**Table 8: Platform Infrastructure**

Feature	What's New
Geo Redundancy	This release introduces the second phase of the geo redundancy solution for Crosswork Network Controller and its components in case of a region or data center failure.
Dual Stack Support	Crosswork has added support for dual stack (IPv4 and IPv6) within a single cluster installation.
Single VM based Crosswork Network Controller	This release introduces the single VM based Cisco Crosswork Network Controller solution that allows you to leverage the device lifecycle functionalities of Crosswork, and it is deployed using a unified package consisting of Crosswork Infrastructure, Embedded Collectors, and Element Management Functions.

Table 9: Documentation

Feature	What's New?
Documentation	<ul style="list-style-type: none"> • 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. • The Cisco Crosswork Network Controller 7.0 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 7.0 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 7.0.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.

DRAFT COPY