Cisco Crosswork Network Controller 1.0.x Release Notes

First Published: 2020-08-11

This document provides information about Crosswork Network Controller 1.0, including compatibility information, known issues and limitations, and updates since the initial release.

Updates to Crosswork Network Controller 1.0

The following table provides details of updates to Crosswork Network Controller 1.0 since its initial release.

Table 1: Updates to Crosswork Network Controller 1.0

Update Type and Version	Date	Description
Patch: Crosswork Network Controller 1.0.1 For patch installation and activation instructions, see Patch Activation Workflow, on page 5.	2020-08-11	The patch resolves the following bugs: • CSCvu27117: RESTCONF API : 500 error while querying policies on node • CSCvv28848: RESTCONF API : 401 error while trying any restconf API

Product Overview

Crosswork Network Controller is an integrated solution combining Network Services Orchestrator (NSO), Segment Routing Path Computation Element (SR-PCE), and Crosswork applications with a common UI and API. The solution enables you to proactively manage your end-to-end networks and provides intent-based and closed-loop automation solutions to ensure faster innovation, good user experience, and operational excellence.

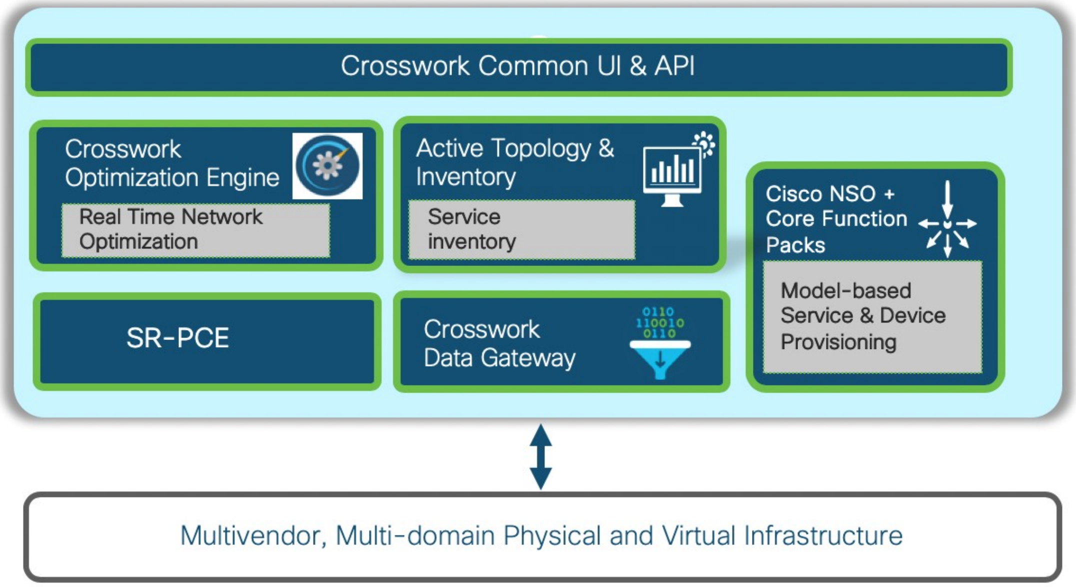
With this integrated solution, you can:

- Visualize network and service inventory on both geographical and logical maps.
- Provision segment routing (SR) traffic engineering policies for services with explicit SLAs by specifying optimization objectives (latency/IGP/TE metric minimization) and constraints (affinities, disjoint paths, bandwidth).
- Provision L2VPN and L3VPN services with associated SLAs.
- Visualize SR policies and VPN services as an overlay on the network topology map.

- Collect realtime performance information and optimize the network to maintain the SLAs. Tactically optimize the network during times of congestion.
- Benefit from realtime bandwidth on demand and bandwidth optimization services.
- Use the APIs to extend the solution based on your specific needs.

The solution is made up of the following components:

Figure 1: Solution Components


Crosswork Common UI & API
Crosswork Optimization Engine
Real Time Network Optimization
Active Topology & Inventory
Service inventory
Cisco NSO + Core Function Packs
Model-based Service & Device Provisioning
SR-PCE
Crosswork Data Gateway
0110
110010
0110
Multivendor, Multi-domain Physical and Virtual Infrastructure

Compatibility Information

Table 2: Solution Component Product Versions

Product	Version
Crosswork Network Controller	1.0
Cisco Crosswork Data Gateway	1.1.2
Cisco Network Service Orchestrator	5.2.2 with Core Function Pack 1.0.0 or greater

Table 3: Cisco IOS XR Software Versions

SR-PCE Software Version	PCC Software Version (Headend Routers)				
	Cisco ASR 9000	**Cisco NCS 5500 series**	**Cisco NCS 540 series**	**Cisco NCS 560 series**	**Cisco XRv 9000**
6.6.3 + SMU[1]	6.5.3 + SMU (CSCvp83001) 6.6.3 + SMU See footnote 1	6.5.3 + SMU (CSCvp83001)[2] 6.6.3 + SMU See footnote 1 and 2	6.6.3 + SMU [3] See footnote 1	6.6.3 + SMU See footnote 1	6.5.3 + SMU (CSCvp83001) 6.6.3 + SMU See footnote 1

[1] 6.6.3 + SMU is needed to support RSVP-TE tunnel and updated SR policy features. SMU file is <platform-name>-6.6.3-Optima.tar.

[2] This SMU is available via the Cisco NCS 5508 Software Download Center.

[3] This SMU is available via the Cisco NCS 540-ACC-SYS Router or Cisco NCS 540x-ACC-SYS Router Software Download Center.

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

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. The correct SMUs to download will have "Optima" or the bug ID appended to the filename. For example:

- **`asr9k-x64-6.6.3.Optima.tar`**
- **`asr9k-x64-6.5.3.CSCvp83001.tar`**

Important Notes

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

- **VPN Service Provisioning:**

  The NSO sample function packs provide example implementations as a starting point for VPN service provisioning functionality in Crosswork Network Controller. The intention is for customers to work with a Cisco Customer Experience representative to adapt these sample function packs to their specific networks and requirements. Although these implementations can be used "as is" to provision flat Layer 2 and Layer 3 VPN services using the GUI or API, they are not guaranteed to be complete and fully tested, and they are not products supported by Cisco.

Known Issues and Limitations

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

Table 4: Known Issues and Limitations

Issue/Limitation	Context within Crosswork Network Controller
Custom templates cannot be created using the GUI, nor can their contents be visualized in the GUI. Custom templates created offline can be applied to service models via GUI and API. However, topology map overlays and service configuration views will not display custom template configuration.	Provisioning GUI.
Demand deduction is not supported in Crosswork Network Controller.	
The Optimization Engine GUI shows TE metric type instead of Latency metric type for SR policies created from the Optimization Engine GUI with Latency as the metric type.	SR policy provisioning from Optimization Engine GUI
After a disaster recovery operation, Crosswork Network Controller must be re-registered with the Cisco licensing server.	**Admin** > **Smart Licensing Registration**
Cisco Crosswork Data Gateway operational state may transition to error state when there is less or no traffic for an extended period of time. Operational state will be updated once the traffic returns to normal levels.	**Admin** > **Data Gateway Management**
The error, "Get Dense Table Operation" may be shown in the Collection Job UI for the SNMP collection type when a large number of devices (300+) are reloaded in an environment. SNMP collection can be resumed by rebooting the Cisco Crosswork Data GatewayVM from the Troubleshooting menu in Cisco Crosswork Data Gateway.	Cisco Crosswork Data Gateway
Services can be provisioned to devices when devices are not mapped to Cisco Crosswork Data Gateway or are operationally down, provided they are reachable and in sync with NSO.	Provisioning GUI
NSO actions such as check-sync, sync-from, re-deploy, reconcile, etc., are not available through the Crosswork Network Controller provisioning UI.	Provisioning GUI

Issue/Limitation	Context within Crosswork Network Controller
After a Cisco NSO backup and restore operation, Crosswork Network Controller discovers all services from Cisco NSO. Any delta in services after the NSO backup operation will be lost once the backup is restored.	Cisco NSO
Crosswork Network Controller can discover services through transit nodes (SR policy, etc.) for non-Cisco vendor devices. These devices will be in Unmanaged state and services cannot be provisioned on these unmanaged devices.	Provisioning GUI
Multiple users performing CRUD operations simultaneously through the Provisioning GUI may encounter failures when one of the sessions is performing bulk operations (e.g., edit route-policy on 100+ devices). NSO configures relevant changes on the network devices and may not respond to subsequent requests in an adequate timeframe, leading to a timeout.	Provisioning GUI
Bulk service operations (create/edit/delete) should be staggered to avoid timeout issues as this is a function of the number of services and overlapping devices.	Provisioning GUI
A device that is also an SR-PCE provider might become unreachable when the device alone is deleted from the Device Management page. To avoid this, add SR-PCE as a provider with a /32 mask.	Device Management, SR-PCE Provider
Segment hops are not visible on the map following multiple add device, delete device, and re-add device operations. Workaround is to restart Optima from **Admin > Crosswork Manager**.	Device Management, Optimization Engine GUI

Patch Activation Workflow

The unit of a patch is a TAR file consisting of the patch metadata, a list of docker images, checksum and signature. The metadata contains platform and product details, patch version, type of patch and other creation details. Signature is a security requirement in order to safeguard the patch; the signature is verified by the patch framework. It also helps to perform error correction mechanisms and detect if the patch is corrupted or not.

Follow the workflow below to add and activate the patch:

1. Download the patch from the Cisco Software Download page and save it on a host that is accessible to the Crosswork VM.

2. **Validate the patch**

API: /crosswork/platform/v1/patch/validate

The patch is validated for accuracy and compatibility to the product version.

3. **Add the patch to the system**

   API: https://<ip or host>:<port number>/crosswork/platform/v1/patch/add

   After the patch is validated, it must be added to the corresponding registry in the system. The Add operation prepares the system for the patch to be activated. This is an asynchronous operation and may take around 15 minutes. Once the Add operation is initiated, a corresponding job ID is received and the operation is performed in the background.

4. **Check status**

   - Check the current status of the patch framework, such as if the Add operation is successful or ongoing, or if the Activate operation has been triggered.

     API: https://<ip or host>:<port number>/crosswork/platform/v1/patch/status

     This will provide the CWPatchID which will be required in order to activate the patch.

   - Check the status of a specific job based on the job ID.

     API: https://<ip or host>:<port number>/crosswork/platform/v1/patch/jobstatus

5. **Activate the patch**

   API: https://<ip or host>:<port number>/crosswork/platform/v1/patch/activate

   After being added to the system, the patch must be activated before any other patch can be added. Activate, like Add, is an asynchronous operation that generates a job ID and is performed in the background. Activation takes the backup of the current state and updates the configuration. If the patch fails, the auto-rollback functionality rolls back to the previous version and the status is updated with the failure details.

   To activate the patch, you must provide the CWPatchId as payload to this API. This CWPatchId can be obtained by invoking the patch status API, as described in the previous step.

   For example, "CWPatchId": "2f718c8d-85e0-4f87-a9f9-5a6bb96b316a"

6. **Get Summary**

   API: https://<ip or host>:<port number>/crosswork/platform/v1/patch/summary

   Provides the overall summary of the patch framework, including the different patch types and patch versions.

   The summary can also be accessed from the GUI. Go to **Admin** > **Crosswork Manager**. You can also verify the health of the system from here.

Note After a reboot of the Crosswork Network Controller VM, the information in both API and GUI reverts to the original release version that was installed, and does not show the patch details. The patch itself remains intact and its functionality is not affected.

To verify that the patch is intact after rebooting the VM:

- **From the GUI:**

  Go to **Admin** > **Crosswork Manager**, locate the application on which the patch was applied, and check the UP time. The UP time should reflect the time the patch was applied as opposed to the time the system was installed.

- **From the CLI:**
  - Log into the Crosswork Network Controller VM.
  - Enter kubectl describe pod <app-name>-XXX | grep Image, where app-name is the application on which the patch was applied. This will show the new patch image.

Removing a Patch

API: https://<ip or host>:<port number>/crosswork/platform/v1/patch/remove

A patch can be removed after it has been added to the system prior to activation, or after it has been activated.

Cisco Bug Search Tool

You can use the Cisco Bug Search Tool to search for a specific bug or to search for all bugs in a release.

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. Use any of these options to search for bugs, and then press Enter (Return) to initiate the search:

   — To search for a specific bug, enter the bug ID in the Search For field.

   — To search for bugs based on specific criteria, enter search criteria, such as a problem description, a feature, or a product name, in the Search For field.

   — To search for bugs based on products, enter or choose the product from the Product list.

   — To search for bugs based on releases, in the Releases list choose whether to search for bugs affecting a specific release, bugs that were fixed in a specific release, or both. Then enter one or more release numbers in the Releases field.

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

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

Related Documentation

Cisco Crosswork Network Controller 1.0 Documentation

The following documents provide usage and other supplemental information for Crosswork Network Controller 1.0. These documents can be accessed on Cisco.com here.

Table 5: Crosswork Network Controller 1.0 Documentation

Document	Description
Crosswork Network Controller 1.0 Release Notes	Provides an overview of the product, compatibility information, and important information that should be taken into consideration before using the product.
Crosswork Network Controller 1.0 Installation Guide	Provides system requirements, installation prerequisites, and installation instructions.
Get Started with Crosswork Network Controller 1.0	Describes the steps required to get up and running with Crosswork Network Controller post-installation.
Manage Transport Services with Crosswork Network Controller 1.0	Describes how to create, provision, and visualize SR-TE policies using Crosswork Network Controller.

API Documentation

See the Cisco Crosswork Network Automation API Documentation on Cisco DevNet.

NSO Core Function Pack Documentation

The following documents provide information about installing and using the Cisco Network Services Orchestration (NSO) Transport SDN Core Function Pack (CFP). These documents can be accessed on Cisco.com here.

Table 6: NSO Core Function Pack Documentation

Document	Description
Cisco NSO Transport SDN Function Pack Bundle Installation Guide Version 1.0.0	Describes how to install the Transport SDN Core Function Pack and sample function packs.
Cisco NSO Transport SDN Function Pack Bundle User Guide Version 1.0.0	Describes how to configure and use the Transport SDN Core Function Pack and sample funtion packs.

Accessibility Features

All product documents are accessible except for images, graphics and some charts. If you would like to receive the product documentation in audio format, braille, or large print, contact the Cisco Accessiblity Team on the Web or send email to accessibility@cisco.com .

Obtain Documentation and Submit a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.