Cisco Crosswork Hierarchical Controller 6.0

Administration Guide

October 2022

Contents

Introduction

This document is an administration guide for configuration of the Cisco Crosswork Hierarchical Controller platform version 6.0. For details on installation, see the *Cisco Crosswork Hierarchical Controller Installation Guide*.

The document explains:

- Security Architecture
- Security and Administration
- System Health
- Database Backup and Restore
- HA Cluster Management
- Device Management (Credentials, Adapters, and Managed Devices)
- Model Settings (Regions, Tags, and Events)
- Link Management

Security Architecture

This section provides information on the security architecture, feature set, configurations, and practices used by Cisco to ensure that Cisco Crosswork Hierarchical Controller is highly secured and can safely be deployed without any risk or vulnerability. Cisco continuously follows the developments and practices commonly accepted by the industry and keeps pace by updating Cisco Crosswork Hierarchical Controller.

This section details the feature set by category, configurations to reduce risks, supported standards, and development and deployment processes. Cisco Crosswork Hierarchical Controller security is based on a layered architecture, where each logical element provides different security, and each security step is a prerequisite for the next one. For instance, user authorization takes place only for users who are already authenticated.

The NGINX Web Server is the only component that is accessible from outside the device on which Cisco Crosswork Hierarchical Controller is installed. The HTTP and SQL connections are internal connections that are bound to local interfaces and are not accessible from outside the device on which Cisco Crosswork Hierarchical Controller is installed. In addition, each logical element runs inside a Docker container, which means that each box is sandboxed and cannot access any of the other boxes or the operating system, except for the explicit connections allowed.

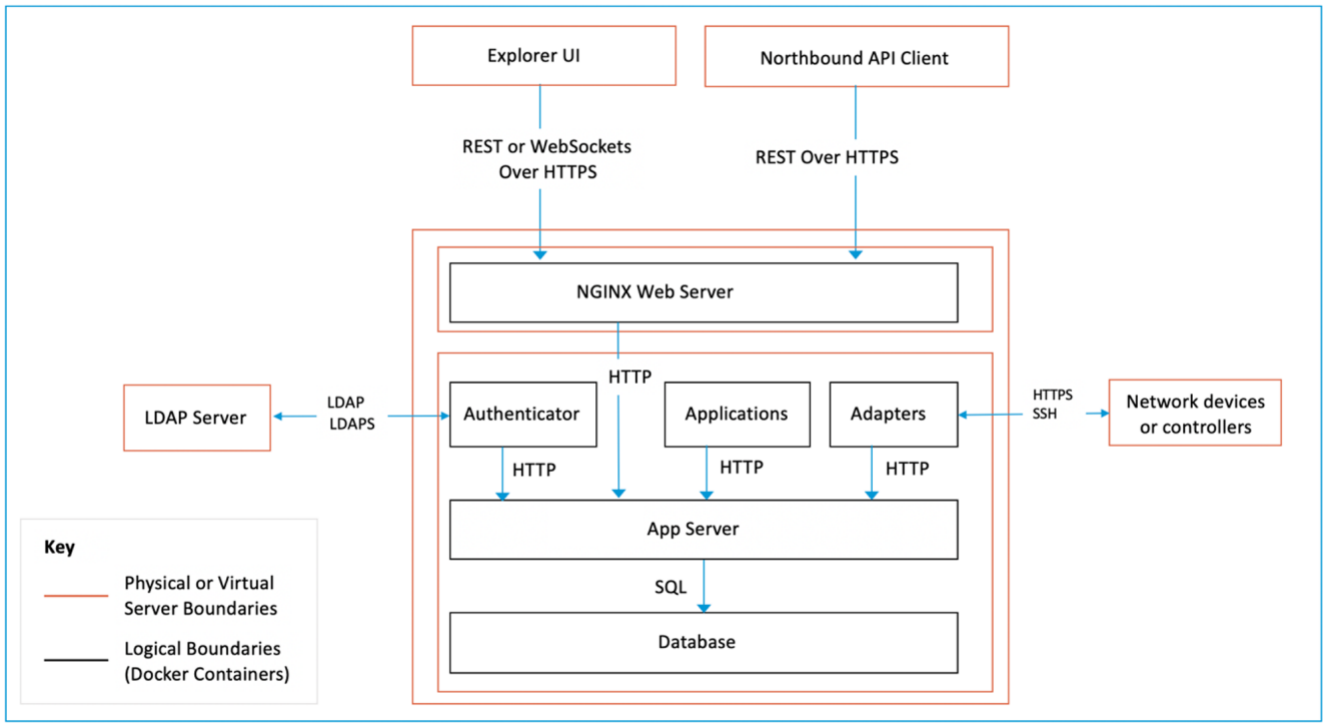


Figure 1.
Cisco Crosswork Hierarchical Controller Security Architecture

Architecture Overview

NGINX Web Server

Cisco Crosswork Hierarchical Controller runs on the App Server deployed behind an NGINX Web Server. The NGINX Web Server is configured as a reverse proxy server, intercepts all requests to the Cisco Crosswork Hierarchical Controller App Server, and acts as the first line of defense against security attacks.

The NGINX Web Server only accepts HTTPS packets on port 443. HTTP traffic is terminated by the reverse proxy and redirected to HTTPS so that HTTP traffic does not reach the Cisco Crosswork Hierarchical Controller App Server.

The NGINX Web Server performs client authorization to the Cisco Crosswork Hierarchical Controller authenticator using the ngx_http_auth_request_module of NGINX.

Authentication Framework

The Cisco Crosswork Hierarchical Controller authentication framework is Passport, an authentication middleware that supports a comprehensive set of authentication strategies.

Password Storage

For local authentication, passwords are stored in the database using secure, salted password hashing that is a one-way function. A salt is random data that is used as input to a function that hashes the password to prevent dictionary attacks. This greatly increases security because passwords are protected even if the password file is compromised.

The hashing function used is bcrypt, which is based on the Blowfish cipher. In addition to incorporating a salt to protect against rainbow table attacks, bcrypt is an adaptive function that ensures Cisco Crosswork Hierarchical Controller remains resistant to brute-force search attacks even with increasing computation power.

Containers

Cisco Crosswork Hierarchical Controller uses Docker containers to deploy and run processes of applications and the Application Server. To maintain a high level of database security, containers are deployed in two separate networks. The Application Server and database are in one network and all the rest of the containers are in another network. Only the Application Server can access the database.

The debug level of containers is initially set to **INFO**.

Database

Cisco Crosswork Hierarchical Controller uses Postgres as the database. Access to the database is restricted by user and password which are kept encrypted. Tables of sensitive data, such as network element details and user credentials, are all encrypted.

Encryption is by AES256.

User Access and Authentication

Cisco Crosswork Hierarchical Controller authenticates users by communicating with an external LDAP server or locally for users defined in Cisco Crosswork Hierarchical Controller.

Each user accessing the system is uniquely authenticated.

Each user can open multiple sessions concurrently.

Cisco Crosswork Hierarchical Controller users can only interact with the platform resources, the user is not able to gain underlying OS access from the platform.

Access management for the host OS and the Cisco Crosswork Hierarchical Controller platform are managed separately.

User Groups

User groups can be defined in the LDAP server, which passes them to Cisco Crosswork Hierarchical Controller upon access accept. These groups are mapped to user roles (see more in Authorization).

Local Users

Cisco Crosswork Hierarchical Controller allows the creation of local users.

As a best practice, locally defined users should be limited to admin users only.

Password Policy Settings

The password strength forced for local users can be enabled or disabled and can be set in scores of 1 to 5 (weak to strong). The given password is checked against several dictionaries and common passwords lists, to ensure its complexity according to the selected score.

Two-factor Authentication

Two-factor authentication is currently not part of the default package; however, it can be added as a professional service on demand.

Communication with LDAP Server

The LDAP application protocol is an open, vendor-neutral industry standard for accessing and maintaining distributed directory information services. LDAPS authentication is similar except that its communication is over an encrypted transport connection.

Administrator Options

The administrator can set the login banner.

The administrator can block and unblock active users and set the idle session expiration time.

User Lockout Policy

After a configurable number of unsuccessful login attempts, the user is blocked. The blocking period starts with a low duration and grows with each failed login attempt.

Default number of login attempts is 8.

Login attempts from the user's IP address are not handled during this period.

Authorization

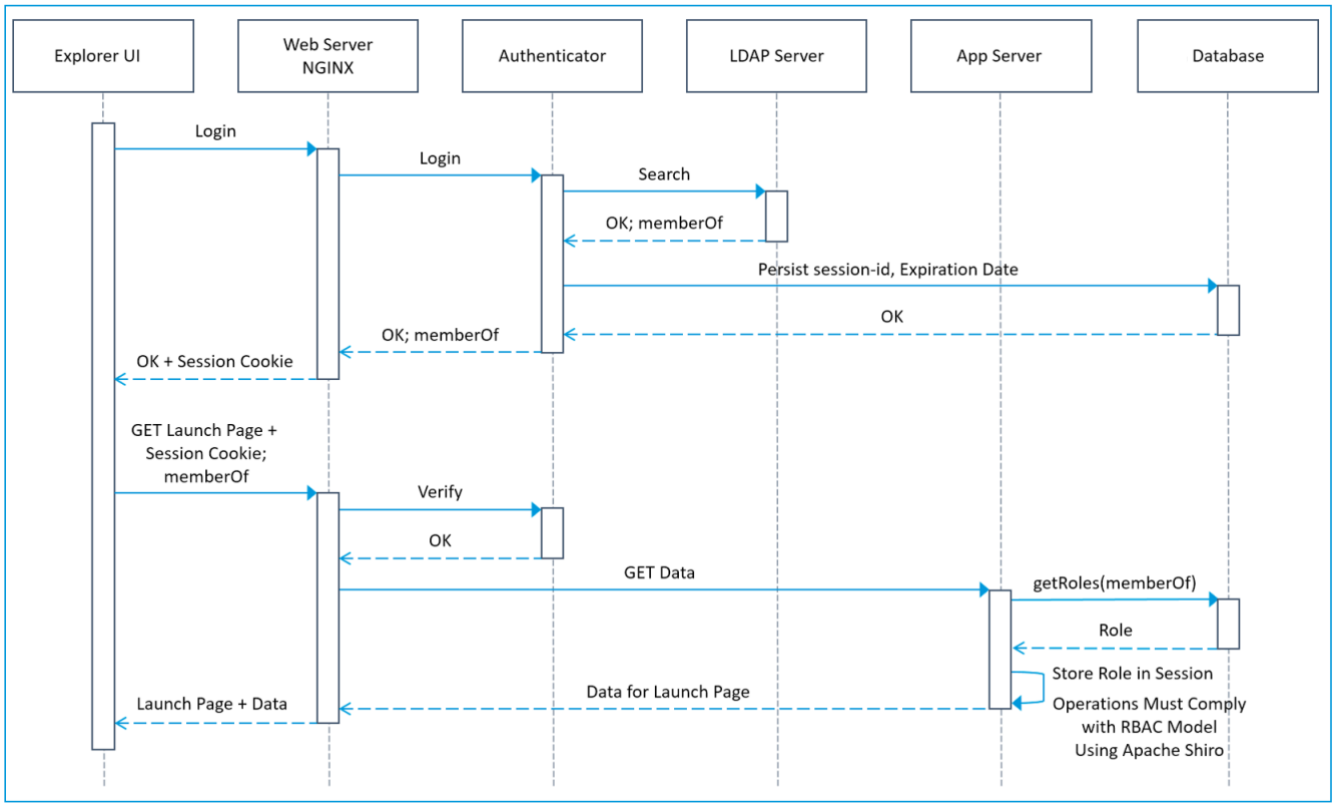


Figure 2.
Cisco Crosswork Hierarchical Controller Authorization Flow

Cisco Crosswork Hierarchical Controller supports role-based access control (RBAC), which enables each user (either locally defined or an LDAP user) to be individually assigned to a role. The following Cisco Crosswork Hierarchical Controller roles are available:

Cisco Crosswork Hierarchical Controller Role	Permissions
Read Only	Read-only access to Cisco Crosswork Hierarchical Controller Explorer UI.
User	Access to Cisco Crosswork Hierarchical Controller Explorer UI and all apps, some of which can change the network.
Administrator	Full control over configuration and all users. Access to Configuration UI, Cisco Crosswork Hierarchical Controller Explorer UI, and all apps.
Support	Same permissions as the User role with the addition of access to Cisco Crosswork Hierarchical Controller diagnostic tools for the Cisco Support Team.

Role Assignment to User

A Cisco Crosswork Hierarchical Controller administrator provides Cisco Crosswork Hierarchical Controller a Bind DN and password that Cisco Crosswork Hierarchical Controller then uses to connect and query the LDAP server. The administrator also configures the search base, search filter, and mapping between LDAP groups and Cisco Crosswork Hierarchical Controller roles. This mapping policy identifies who can log in to the Cisco Crosswork Hierarchical Controller Explorer UI and which role they have. All users that meet both the search base and the search filter criteria are permitted to log in with the roles (access privileges) assigned to their group. If the user is not a member of any group that is mapped to a Cisco Crosswork Hierarchical Controller role, the login attempt is rejected.

The Cisco Crosswork Hierarchical Controller administrator also assigns roles to local users who are not handled by LDAP. Both local users and access to the LDAP server can be disabled so that one or the other method can be used for authentication and authorization.

Access to VM and Containers

VM Level

Cisco Crosswork Hierarchical Controller is installed in several micro-services installed on Docker containers hosted on any VM with the proper OS version and HW resources allocated.

Access restriction at the VM OS level is the responsibility of the operator.

Communication via the host OS to Cisco Crosswork Hierarchical Controller is with encrypted protocols - HTTPS/WS secure for UI/NBI and SSH for advanced management via host OS.

Open only the following specific ports in the VM for Cisco Crosswork Hierarchical Controller as listed here:

Direction	Port	Description
Inbound	TCP 22	SSH remote management
	TCP 80	HTTP for UI access (redirect to HTTPS)
	TCP 443	HTTPS for UI access
Outbound	TCP+ 22	NETCONF to routers
	UDP 161	SNMP to routers and/or ONEs
	TCP 389	LDAP if using Active Directory
	TCP 636	LDAPS if using Active Directory
	Customer Specific	HTTP for access to an SDN controller
	Customer Specific	HTTPS for access to an SDN controller

Access to the VM and to the NGINX Server can be restricted to specific IP addresses and ports (white list) during the initial installation.

Containers

Cisco Crosswork Hierarchical Controller uses Alpine OS for containers, it only uses one port and listens to localhost.

HTTP Access in Northbound Interface

The Cisco Crosswork Hierarchical Controller management interface uses secured interfaces. HTTPS/Secure WebSocket is used on the management interface for application-level management for both the GUI and NBI.

Web access to Cisco Crosswork Hierarchical Controller UI and to Web services (REST commands) is protected with SSL and a certificate in X509 version 3.

The URL does not include any user credentials or device-sensitive information.

Access in Southbound Interface

All control traffic between Cisco Crosswork Hierarchical Controller and NEs/NMSs is encrypted.

This is dependent on the NE/NMS ability to provide encrypted interface. As a best practice policy, Cisco will choose the most secure interface/protocol the NE/NMS has to offer.

Audit Trail Log (Accounting)

All user login/logout and operations activities in applications are audited, logged and can be exported to external systems. The audit log contains the username, hostname, time, operation, specific information, and results.

Events and Notifications

System events are stored in Cisco Crosswork Hierarchical Controller DB and can be accessed via SHQL command. This includes:

- Login/logout sessions
- Applications activities
- Updates in network inventory and topology

Events can be sent as SYSLOG to multiple destinations according to their category.

EU Data Protection Directive

As a network controller, Cisco Crosswork Hierarchical Controller deals with network data, and does not deal with data associated with a 'natural person' as defined within GDPR, as outlined by the EU data protection directive. Moreover, Cisco is at most the data processor when addressing support tickets, the Service Provider customer remains the data controller, and data processor, utilizing Cisco Crosswork Hierarchical Controller. There is no personal data associated with a 'natural person'.

Development Security Procedures

Cisco's continuous integration build process runs a static check, including security checks. Static analysis does not allow the build to continue if there are high-severity warnings, such as security warnings. The continuous integration process also runs a Web Server scanner on an instance of Cisco Crosswork Hierarchical Controller that is automatically deployed for integration test purposes.

The security tools, which are referenced by OWASP[1], are FindBugs, Find Security Bugs plug-in and Test-ssl that verifies SSL configuration.

- FindBugs is an open-source tool that uses static analysis to detect bug patterns in Java code. Potential errors are ranked, enabling developers to readily understand the possible impact or severity. One of the main techniques FindBugs uses is to syntactically match source code to known suspicious programming practice.
- Find Security Bugs is a FindBugs plugin for security audits of Java Web applications. It can detect 86 different vulnerability types with over 200 unique signatures. Extensive references are given for each bug pattern with references to OWASP Top 10 and CWE2.
- Test-ssl is a command line tool which checks a server's service on any port for the support of TLS/SSL ciphers, protocols as well as recent cryptographic flaws and more

Security Patches Update Policy

Cisco is responsible for ensuring that all software libraries and images, used by the Cisco Crosswork Hierarchical Controller software and by its deployment components, are all fully protected against any security threats, and do not generate any malware or virus risk to other systems in the service provider network.

Active Engagement to Secure Cisco Crosswork Hierarchical Controller Software

To meet this commitment, Cisco performs the necessary steps, as described in this document, to comply with this statement. Steps are taken in the design phase, when selecting new component and certify it before use, when any upgrade is required to such components, and when security patches are proactively being released. These tests, using Clair, check for vulnerabilities in containers.

---

[1] OWASP (Open Web Application Security Project) is an organization that focuses on Web application security. One of its endeavors is to publish a list of the top 10 vulnerabilities.

[2] CWE (Common Weakness Enumeration) is an international organization that provides a unified, measurable set of software weaknesses.

New Software Component Certification

The use of any software library or image by Cisco Crosswork Hierarchical Controller, its containerized host, databases, and operating system is subject to security certification by Cisco as part of its selection, prior to its use.

The certification process ensures by reviewing official declarations and by testing that it stands in following conditions:

- Ports in use are well-known.
- Any communication is by secured protocols (SSH, HTTPS, TLS v1.2/1.3) with certification, SFTP).
- No use of super user or admin privileges.
- Authentication is required to access its APIs.
- Authorization is implemented internally between processes.
- Password rules are enforced.
- Security test results are published.

Cisco always prefers software libraries and product with the highest security level. In case no substitute software is available, it will make careful use of it by restricting its use and will notify in release notes of any potential risk that may be caused by this software.

Proactive Patches Update Policy

Cisco continuously tracks the relevant opensource software libraries and enterprise software products in use or that interact with Cisco Crosswork Hierarchical Controller. The full list can be retrieved from Cisco if required.

The purpose of the tracking is to find if there are any patch updates or alerts related to security holes or threats caused by this software to its users.

Cisco experts examine the potential risk by its use in Cisco Crosswork Hierarchical Controller and decide on the severity and the actions to take. Based on its urgency level, it may be decided to perform the following:

- In case of alert – generate an official information letter to all its deployed customers. Such a letter notifies customers that Cisco is aware of the situation and is committed to resolve the matter with the release of a patch. In cases where no recovery is planned, Cisco may consider a replacement of the component.
- When a patch is released – in case the threat repaired by the patch was found to have an impact on Cisco Crosswork Hierarchical Controller users. Cisco will start the process of a patch update. This process involves; 1) upgrade to the patch in R&D lab, 2) proper quality tests to ensure its smooth operation with no harm to security and to Cisco Crosswork Hierarchical Controller functionality, 3) release of the patch as a formal notification to all Cisco Crosswork Hierarchical Controller users. The formal notification on patch upgrade may, upon its severity, be received electronically or personally.

Reactive Patches Update Policy

On very rare occasions, a security threat may be found by Cisco Crosswork Hierarchical Controller users who will alert Cisco.

Cisco is fully committed to act immediately and assess the impact of the reported threat on its software and environment. Cisco will share the results with the customer and will take the necessary steps to avoid any damage. Steps may require a Cisco Crosswork Hierarchical Controller patch upgrade. In this case, Cisco will inform the user whether an independent upgrade using the security patch by the user is permitted.

Testing

Security patches of any software component are tested against Cisco Crosswork Hierarchical Controller to ensure that they have no effect on any of the functionality. If there is any resulting limitation, this will be reported in the patch release notes.

Approval

Following the test results and based on the assessment of risks to software stability and quality, the patches deliveries are reviewed by security and IT team in charge and approval is given to the field team to proceed with the installation. Approval is a formal part of the delivery, and it states the approvers names in the path release notes

Delivery

Delivery of patches, for security and for any other purpose, is followed by a formal notification by Cisco to all its users. Security patches are declared as such, they are released with proper documentation, and are free and not connected to any specific maintenance agreement.

Note that upgrades to the latest security patches are mandatory to ensure continuous support by Cisco, as per the maintenance agreement, and when upgrading to a newer version of Cisco Crosswork Hierarchical Controller.

Security and Administration

Install a Certificate

Getting a valid certificate is a two phase process. First, generate a Certificate Request (CSR), then, this file is used by the CA (Customer IT team) to generate a trusted certificate (PEM/CRT) to be installed on the server.

Before generating the CSR, you'll need the exact URL of the deployed system, e.g: cisco.corp.com. This is the certificate Common Name (CN).

To generate a CSR:

1. Access the Cisco Crosswork Hierarchical Controller server's command line (usually using SSH).
2. Ensure that you are logged in as root. If you logged in as a different user, run:
   ```
   sudo su -
   ```
3. Create a folder for the CSR:
   ```
   mkdir /usr/local/etc/sedona/ssl
   ```
4. Change path to the folder created:
   ```
   cd /usr/local/etc/sedona/ssl
   ```
5. Generate a new DH param file (this may take a few minutes):
   ```
   openssl dhparam -out dhparam.pem 2048
   ```

To install the certificate:

1. Copy the PEM file received from the CA into `/usr/local/etc/sedona/ssl/new_certificate.pem`.
2. Restart the system:
   ```
   sedo system restart
   ```

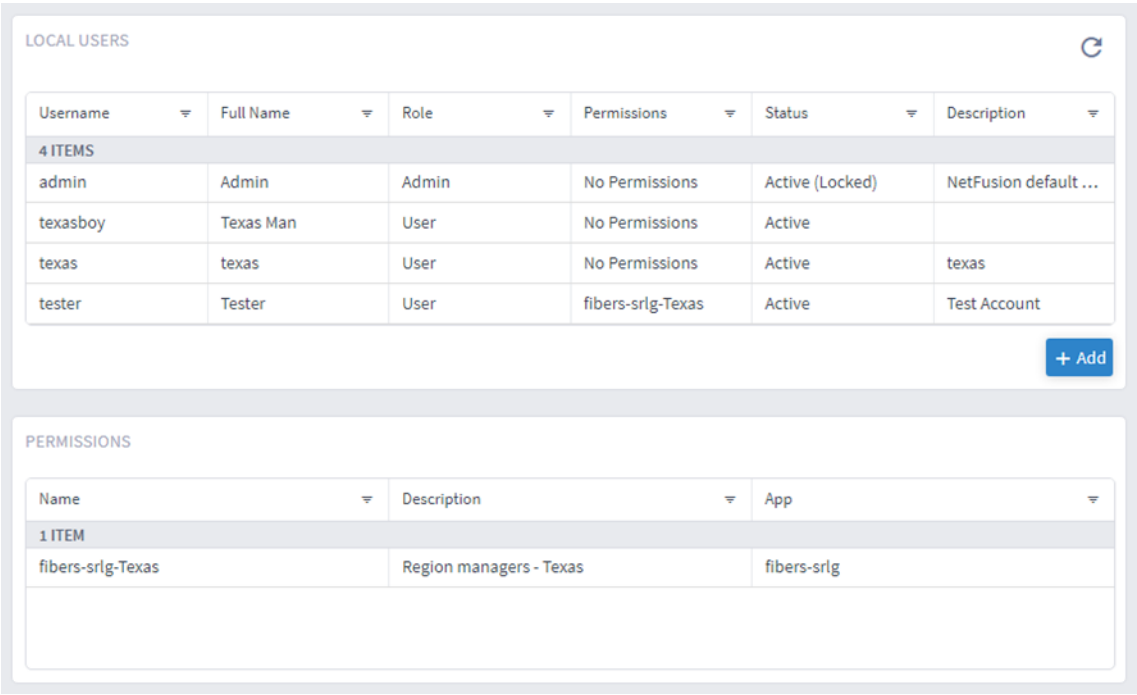
User Administration

Crosswork Hierarchical Controller supports the creation and maintenance of local users, as well as integration with an Active Directory (LDAP) server. Local users can be created and assigned a role and permissions. The administrator can also select password complexity rules (OWASP) on passwords of local users. By selecting a scoring level, the length and character composition of the password is enforced.

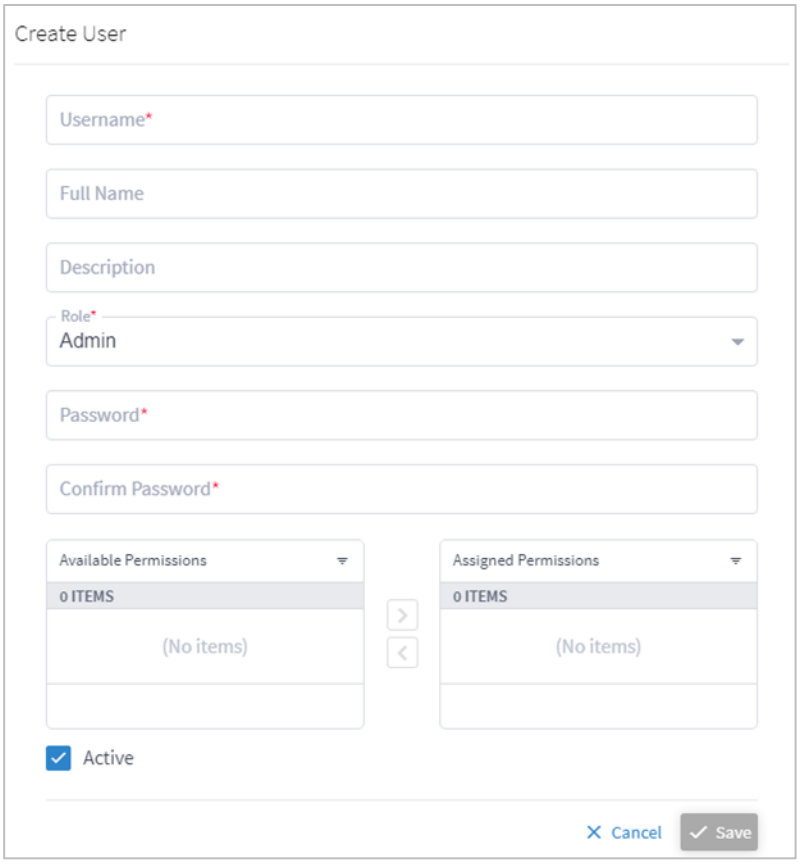
Crosswork Hierarchical Controller Role	Permissions
ReadOnly	Read-only access to Crosswork Hierarchical Controller Explorer UI.
User	Access to Crosswork Hierarchical Controller Explorer UI and all apps, some of which can change the network.
Admin	Full control over configuration and all users. Access to Configuration UI, Crosswork Hierarchical Controller Explorer UI, and all apps.
Support	Same permissions as the User role with the addition of access to Crosswork Hierarchical Controller diagnostic tools for the Cisco Support Team.

To add/edit a user:

1. In the applications bar in Crosswork Hierarchical Controller, select **Settings**.
2. Click **Security Settings**.



3. In **LOCAL USERS**, click **Add** or click on an existing user.



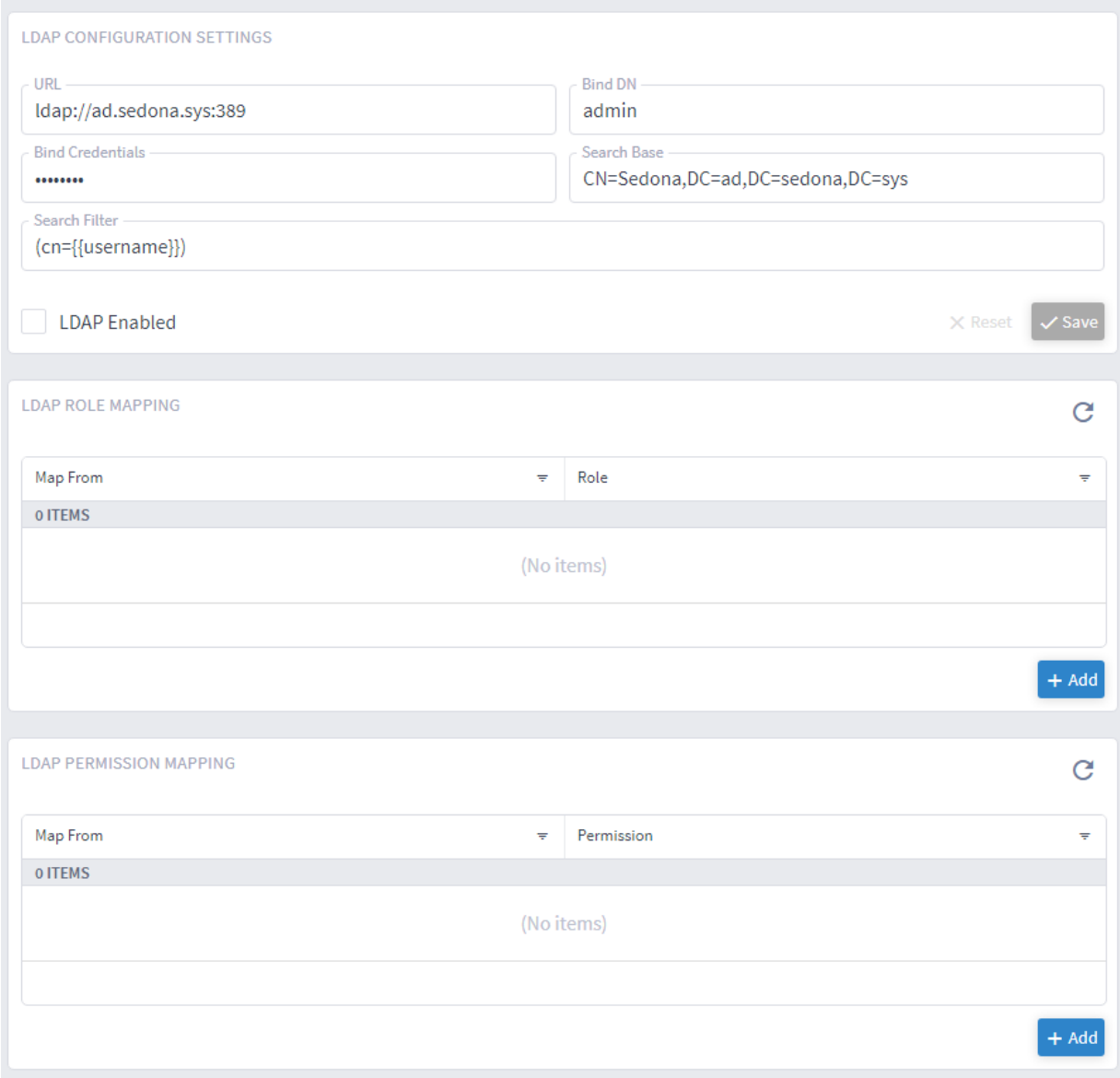
4. Complete the fields and assign any required permissions.
5. Click **Save**.

Active Directory

Crosswork Hierarchical Controller allows for authenticating users via an LDAP server.

To configure an LDAP Server:

1. In the applications bar in Crosswork Hierarchical Controller, select **Settings**.
2. Click **Security Settings**.



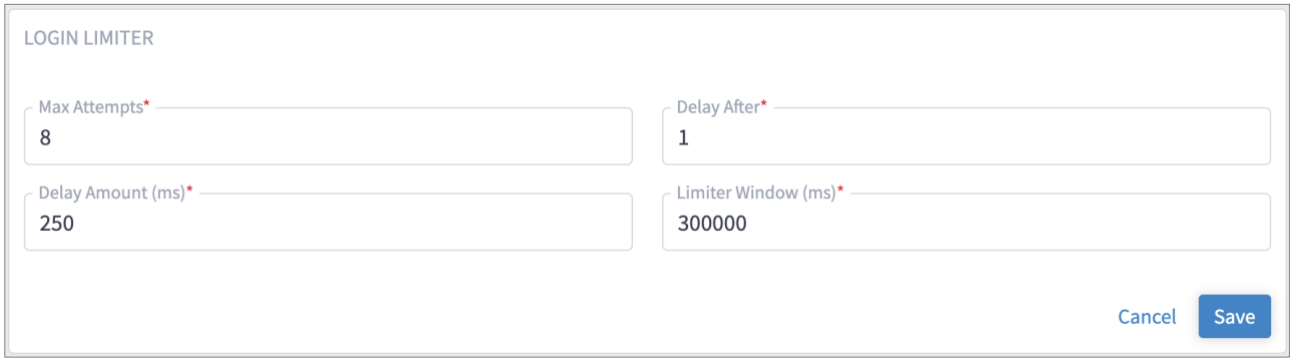
3. Configure the **ACTIVE DIRECTORY (LDAP)** settings.
4. Click **Save**.

Login Limits

The number of logins attempts by users can be limited to avoid denial of service and brute force attacks.

To configure login limits:

1. In the applications bar in Crosswork Hierarchical Controller, select **Settings**.
2. Click **Security Settings**.



3. Configure the **LOGIN LIMITER** settings.
   - **Max Attempts:** The maximum number of login attempts.
   - **Delay After:** The number of incorrect login attempts before the delay is applied.
   - **Delay Amount (ms):** The time in ms before the next login attempt is permitted.
   - **Limiter Window (ms):** The period when login is not permitted once the max attempts are exceeded. Usually set to 300000 ms or 5 minutes.
4. Click **Save**.

SYSLOG Notifications

Crosswork Hierarchical Controller can send SYSLOG notification on security and monitoring events to multiple destinations.

The categories of these events are:

- **All** – security and monitoring
- **Security** – all login and logout events
- **Monitoring** – disk space thresholds, load average thresholds
- **Custom** – custom category events

Crosswork Hierarchical Controller sends three types of messages with the following facility codes:

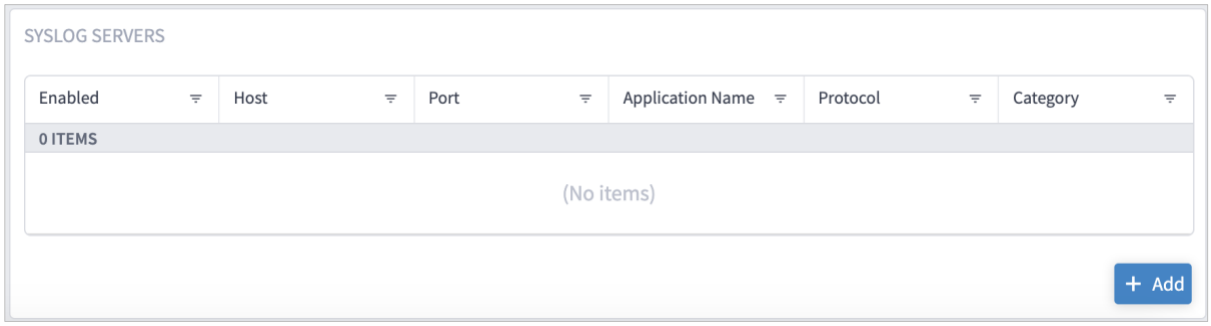
- **AUTH (4)** – for /var/log/security messages.
- **LOGAUDIT (13)** – for Audit messages (login, logout, and so on).
- **USER (1)** – for all other messages.

Crosswork Hierarchical Controller sends Device Manager SYSLOG events when the:

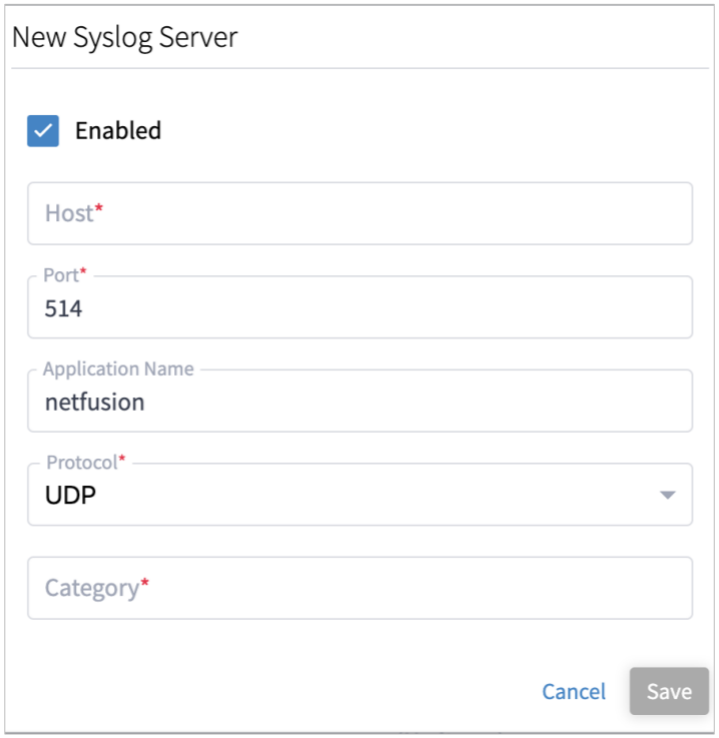
- Device reachability state changes
- Adapter fails to parse files
- Adapter fails to connect to the controller, for example, Authentication failure or TCP Connection failed.

To add a new Syslog server:

1. In the applications bar in Crosswork Hierarchical Controller, select **Settings**.
2. Click **Security Settings**.



3. In **SYSLOG SERVERS**, click **Add**.



4. Complete the following:
   - **Host**
   - **Port:** 514 or 601
   - **Application Name:** free text
   - **Protocol:** TCP or UDP
   - **Category:** All, Monitoring, Security, or Custom

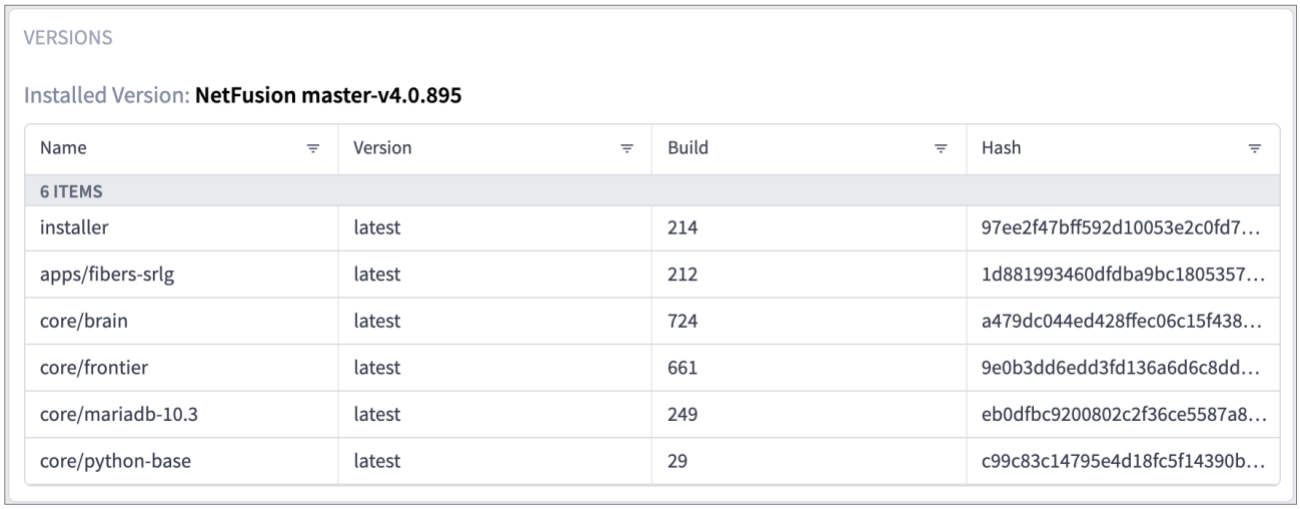
5. If you selected **Custom**, enter a custom category.
6. Click **Save**.

System Health

View System Info

To view system info:

1. In the applications bar in Crosswork Hierarchical Controller, select **Settings**.


VERSIONS

Installed Version: **NetFusion master-v4.0.895**

Name	Version	Build	Hash
6 ITEMS			
installer	latest	214	97ee2f47bff592d10053e2c0fd7…
apps/fibers-srlg	latest	212	1d881993460dfdba9bc1805357…
core/brain	latest	724	a479dc044ed428ffec06c15f438…
core/frontier	latest	661	9e0b3dd6edd3fd136a6d6c8dd…
core/mariadb-10.3	latest	249	eb0dfbc9200802c2f36ce5587a8…
core/python-base	latest	29	c99c83c14795e4d18fc5f14390b…

2. In **System Info**, the **VERSIONS** table displays the installed packages and their build number.

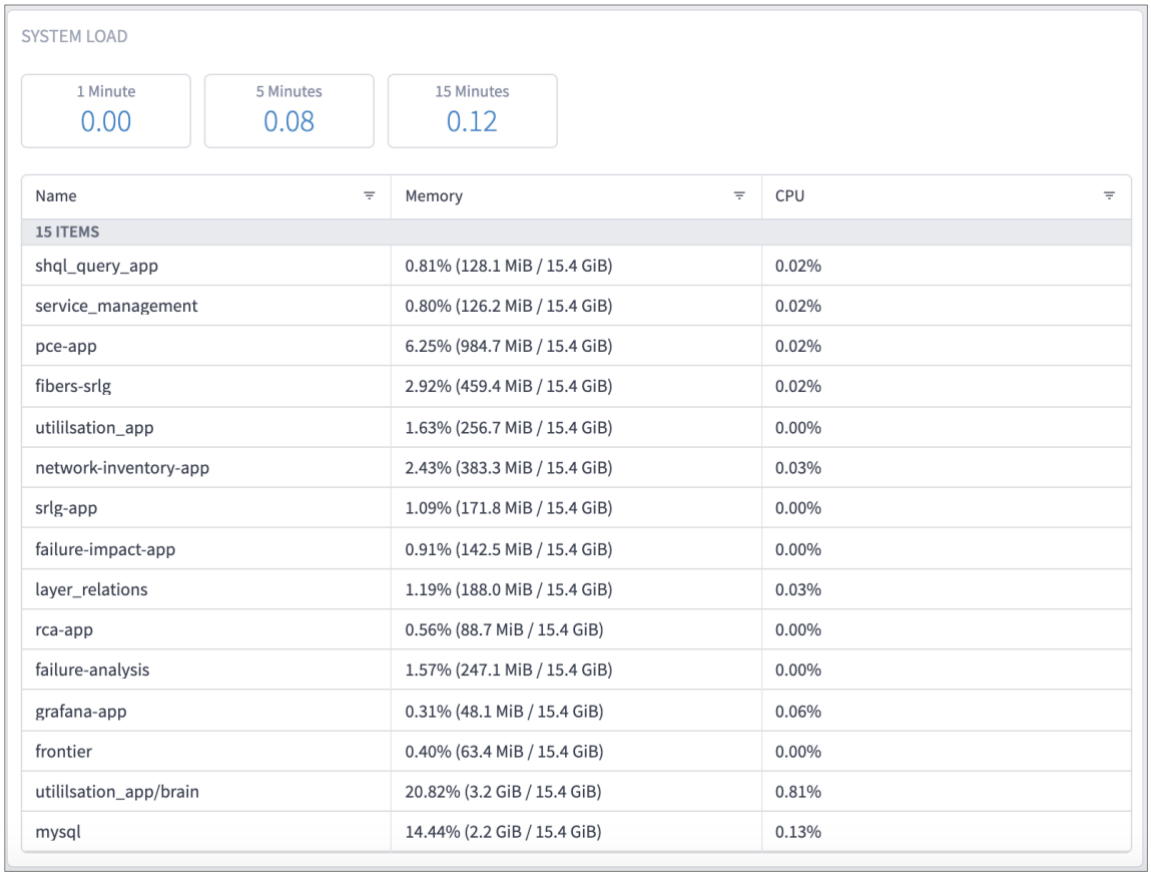
View System CPU Load

The Crosswork Hierarchical Controller platform performance can be tracked, and you can view system CPU load and disk usage in the UI to isolate a specific service that may cause a reduction in performance or block specific functionality.

To view the system load:

1. In the applications bar in Crosswork Hierarchical Controller, select **Settings**.
2. In **System Info**, the **SYSTEM LOAD** information is updated every two minutes by default.
    - The values in the three rectangles displays the percentage of the CPU used by Crosswork Hierarchical Controller in the last minute, 5 minutes and 15 minutes (server load average).

- The columns display the percentage memory and CPU currently used by each of the Crosswork Hierarchical Controller processes.



3. To configure a different interval, run the command:

   ```
   sedo config set monitor.load_average.rate.secs [VALUE]
   ```

4. Refresh the screen to see the change.
5. To set a load average threshold (a SYSLOG notification is generated when this is crossed), run the command:

   ```
   sedo config set monitor.load_average.threshold [VALUE]
   ```

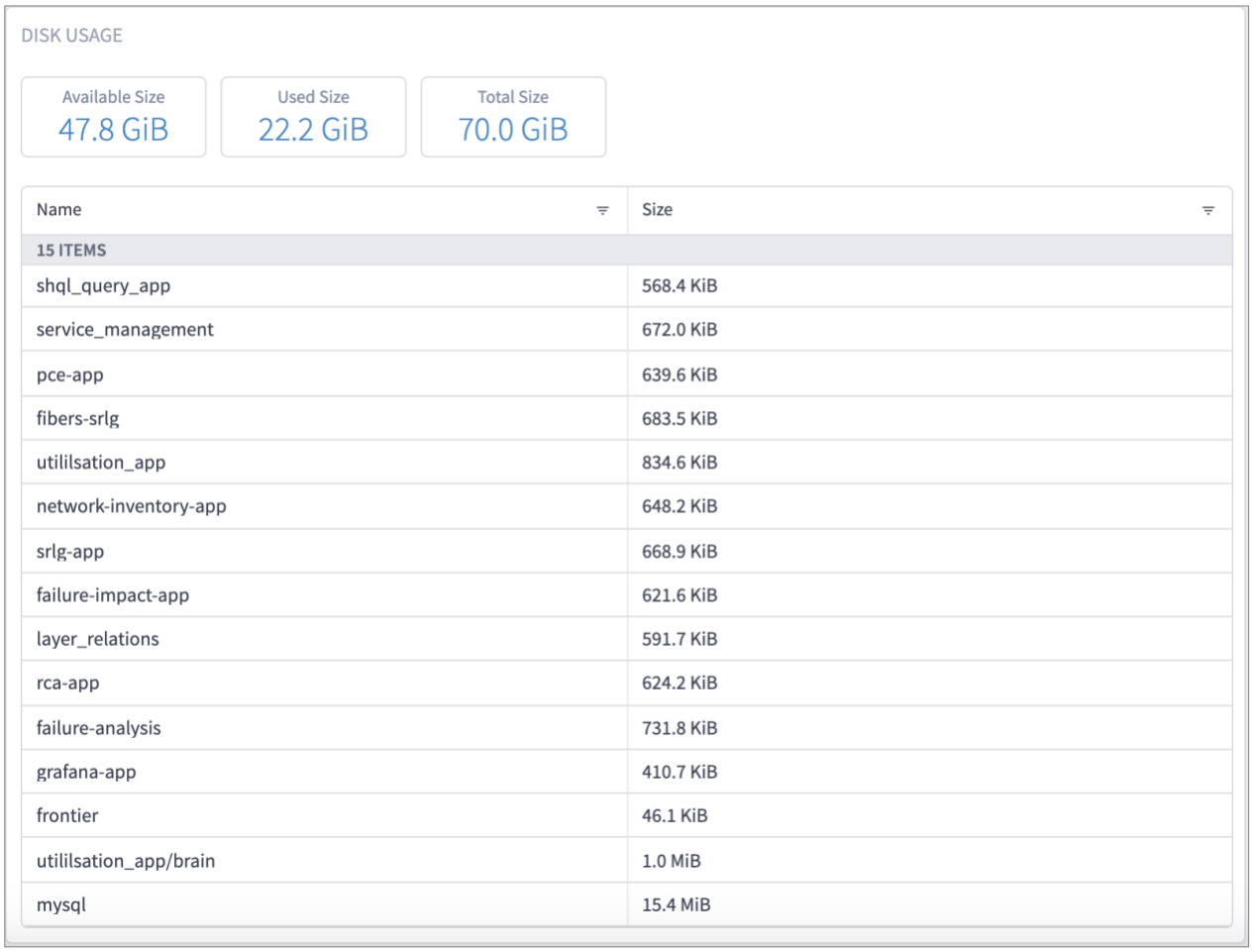
   The recommended threshold is the number of cores multiplied by 0.8.

View Disk Usage

To view disk usage:

1. In the applications bar in Crosswork Hierarchical Controller, select **Settings**.
2. In **System Info**, the **DISK USAGE** information is updated every hour by default.
   - The values in the three rectangles displays the available, used and total disk space on the current partition.

- The Size column displays the size of each of the Crosswork Hierarchical Controller application containers (excluding the application data).



3. To configure a different interval, run the command:

   ```
   sedo config set monitor.diskspace.rate.secs [VALUE]
   ```

4. Refresh the screen to see the change.
5. To set a disk space threshold (a SYSLOG notification is generated when this is crossed), run the command:

   ```
   sedo config set monitor.diskspace.threshold.secs [VALUE]
   ```

   The recommended threshold is 80%.

Crosswork Hierarchical Controller Database Backup and Restore

Periodical Crosswork Hierarchical Controller DB Backup

- Backups are done every day automatically.
- Daily backups only include the gap from the previous day. These delta backups expire after a week.
- A full backup is done once a week automatically. The full backup expires after a period, which by default is set to a year.

Backup Commands

```
sedo backup [-h] COMMAND …
```

positional arguments:

```
COMMAND
     create     create a backup
     list       list available backups
     export     export a backup to file
     delete     delete backups
```

optional arguments:

```
-h, --help show this help message and exit
```

Manual Crosswork Hierarchical Controller DB Backup

You can manually back up the database, and you can use this complete backup file to restore the Crosswork Hierarchical Controller database or copy it to a new instance.

To back up the DB:

- To back up the database, use the command:

```
sedo backup create [-h] [--omit-stats] [-f] [FILENAME]
```

positional arguments:

```
FILENAME   specify filename (default: netfusion-backup-<version>-<timestamp>.tar.gz)
```

optional arguments:

```
-h, --help      show this help message and exit
--omit-stats    omit the operational statistics table (not for production use!)
-f, --force     do not prompt for confirmation
```

The backup file name includes the version and date.

Restore the Crosswork Hierarchical Controller DB

When you restore, Crosswork Hierarchical Controller uses the last full backup plus the delta backups to restore. This is done automatically for you when you use the restore command.

To restore the DB:

- To restore the database, use the command:

```
sedo system restore [-h] (--backup-id BACKUP_ID | --filename FILENAME) [--no-verify] [-f]
```

optional arguments:

```
-h, --help                show this help message and exit
--backup-id BACKUP_ID     restore backup by this ID
--filename FILENAME       restore from this backup filename
--no-verify               do not verify backup file integrity
-f, --force               do not prompt for confirmation
```

List the Crosswork Hierarchical Controller DB Backups

Backups are created as follows:

- A full backup is created every Sunday (with an expiration of a year later, by default).
- A delta backup is created daily, except for Sunday (with an expiration of seven days later).

So typically you will see six delta backups between full backups.

In addition, full backups are created (with an expiration of seven days later):

- When the machine is first installed.
- If Crosswork Hierarchical Controller or the entire machine is rebooted (Monday to Saturday).

To list the backups:

- To list the backups, use the command:

  ```
  sedo backup list[-h]
  ```

  optional arguments:

  ```
  -h, --help      show this help message and exit
  ```

```
+----+--------+-----------------------+--------+-----------------------+----------+----------+
|    | ID     | Timestamp             | Type   | Expires               | Status   | Size     |
+====+========+=======================+========+=======================+==========+==========+
|  1 | QP80G0 | 2021-02-28 04:00:04+00 | FULL   | 2022-02-28 04:00:04+00 | OK       | 75.2 MiB |
+----+--------+-----------------------+--------+-----------------------+----------+----------+
|  2 | QP65S0 | 2021-02-27 04:00:01+00 | DELTA  | 2021-03-06 04:00:01+00 | OK       | 2.4 MiB  |
+----+--------+-----------------------+--------+-----------------------+----------+----------+
|  3 | QP4B40 | 2021-02-26 04:00:04+00 | DELTA  | 2021-03-05 04:00:04+00 | OK       | 45.9 MiB |
+----+--------+-----------------------+--------+-----------------------+----------+----------+
|  4 | QP2GG0 | 2021-02-25 04:00:03+00 | DELTA  | 2021-03-04 04:00:03+00 | OK       | 44.3 MiB |
+----+--------+-----------------------+--------+-----------------------+----------+----------+
|  5 | QP0LS0 | 2021-02-24 04:00:00+00 | DELTA  | 2021-03-03 04:00:00+00 | OK       | 1.5 MiB  |
+----+--------+-----------------------+--------+-----------------------+----------+----------+
|  6 | QOYR40 | 2021-02-23 04:00:03+00 | FULL   | 2021-03-02 04:00:03+00 | OK       | 39.7 MiB |
+----+--------+-----------------------+--------+-----------------------+----------+----------+
```

Delete Backup

You can delete backups in a specific time frame. To delete a single backup, set the FROM_ID to the same value as the TO_ID.

Deleting a full backup also deletes the successive delta backups.

To delete a backup:

- To delete a backup, use the command:

  ```
  sedo backup delete [-h] [-f] FROM_ID TO_ID
  ```

  positional arguments:

```
FROM_ID    delete backups starting from this backup ID inclusive
TO_ID      delete backups up to this backup ID inclusive
```

optional arguments:

```
-h, --help      show this help message and exit
-f, --force     do not prompt for confirmation
```

Export Backup

You can export a backup to a file.

To export a backup:

- To export a backup, use the command:

  ```
  sedo backup export [-h] BACKUP_ID [FILENAME]
  ```

  positional arguments:

  ```
  BACKUP_ID  export backup of this ID
  FILENAME   specify filename (default: netfusion-backup-<version>-<timestamp>.tar.gz)
  ```

  optional arguments:

  ```
  -h, --help      show this help message and exit
  ```

HA Cluster Management

Deconfigure HA Cluster

To deconfigure the HA cluster, disconnect the nodes from the HA cluster in the following order:

- Standby
- Witness
- Active (Leader)

By default, when you uninstall the apps are disabled. You can keep the apps on the active node and continue running on a single node.

To deconfigure the HA cluster:

1. On the standby node, run the following command:

   ```
   sedo ha reset-node
   ```

2. To confirm that you want to disconnect the current node (standby) from the HA cluster, type:

   ```
   Y
   ```

3. Repeat to disconnect the witness node.
4. To disconnect the Leader (active) node and keep the applications running, run the following command:

   ```
   sedo ha reset-node –keep-apps
   ```

5. To check the state of the cluster, run the following command:

   ```
   sedo ha state
   This node is not part of a cluster.
   ```

Upgrade HA Cluster

To upgrade the HA, deconfigure the HA cluster, upgrade the nodes, and then reassemble the cluster.

To upgrade the HA cluster:

1. Deconfigure the cluster. See Deconfigure HA Cluster.
2. Upgrade each of the nodes.
3. Configure the cluster. See the *Cisco Crosswork Hierarchical Controller Installation Guide*.

Restore HA Cluster

Use the desired backup to restore the cluster.

Note: Only restore a backup from the same version.

To restore the HA cluster:

1. Deconfigure the cluster. See Deconfigure HA Cluster.
2. Restore one node using the desired backup (from one of the instances). The database on this node will be the basis for the cluster.
3. Configure the cluster from this restored node. See the *Cisco Crosswork Hierarchical Controller Installation Guide*.

Check HA State

The state command returns the IPsec Tunnels, etcd Nodes and Database cluster info.

To check the state of the HA cluster:

- Run the following command to see the state of the HA cluster:

  ```
  sedo ha state
  ```

  The nodes are connected via a full mesh of IPsec tunnels and have a distributed datastore for persistent cluster configuration using the etcd tool.

Device Management

Terminology

Term	Definition
Adapter	The software used by Crosswork Hierarchical Controller to connect to a device or to the manager, in order to collect information required by the network model and configure the device.
Device	Optical network element, router, or microwave device.
Device Manager	The Crosswork Hierarchical Controller application that manages the deployed adapters.
NMS	Network Management System. Manages multiple optical network elements or routers.
SDN Controller	Software that manages multiple routers or optical network elements.

About Device Management

A key need for operators is network discovery and the monitoring and management of network devices. This is achieved by configuring network adapters to monitor groups of network devices, either directly or by using their management systems (EMS, NMS, or SDN Controller), using various technologies, such as CLI, SNMP or REST.

The Device Manager is a crucial Crosswork Hierarchical Controller application that manages Crosswork Hierarchical Controller southbound adapters, enabling you to add and manage devices, manage the assignment of devices to an adapter and monitor the adapter's health as well as the devices reachability and discovery states.

Device Manager enables you to start discovering the network, monitor the connectivity and troubleshoot when a connectivity failure occurs.

The Device Manager service is available both in the UI and as an API.

To accurately reflect reachability and discovery, the Device Manager application provides the device discovery status per adapter and per information type (inventory, topology, and statistics). In 3D Explorer, the device **Reachability Status** is an aggregated state that reflects the state of all information types.

Crosswork Hierarchical Controller sends SYSLOG events when the:

- Device reachability state changes
- Adapter fails to parse files
- Adapter fails to connect to the controller, for example, Authentication failure or TCP Connection failed.

Credentials

When you work with adapters you are required to use credentials. These are used for authentication when a device is assigned to an adapter. The same credentials may be shared by multiple adapters. You can therefore create "template" credentials for reuse. For ease of use, ensure that you enter a meaningful name.

You can add, edit, and delete credentials.

A credential can be one of the following:

- SSH User and Password
- SSH Public Key
- HTTP
- SNMP Community
- SFTP

Add Credential

You can add a credential.

To add a credential:

1. In the applications bar in Crosswork Hierarchical Controller, select **Services > Device Manager**.
2. Select the **Credentials** tab.
3. Click **Add new credentials**.
4. Enter the **Name** and select a **Type**.
5. Enter the required credentials.
6. Click **Add Credentials**.

Delete Credential

You can delete a credential.

To delete a credential:

1. In the applications bar in Crosswork Hierarchical Controller, select **Services > Device Manager**.
2. Select the **Credentials** tab.
3. Select the required credential.
4. Click **Delete selected credentials**. A confirmation message appears.
5. Click **Confirm**.

Adapters

Adapter types are installed by Cisco. An adapter type uses a specific protocol to manage a specific scope of information to be retrieved or configured on a group of devices or network manager. An adapter type connects to one manager only, for example, an EPN-M instance.

An adapter is an instance of an adapter type and is used by Crosswork Hierarchical Controller to connect to a device or to the manager, to collect information required by the network model and configure the device.

The Device Manager manages the deployed adapters, the assignment of devices to adapters and managers and the status of both adapters and devices throughout the lifecycle of operations. An adapter once configured to connect to devices and/or a manager, polls periodically to make sure that the devices and/or the NMS are reachable and discovered.

Note: The discovery state of the links is reported in Explorer and in the Network Inventory application (not in the Device Manager).

A device or manager may be associated with one or more adapters. This means that you can monitor the same device for different types of information by associating the device with multiple adapters.

All adapters accessing a device or manager, use the same IP address or host name, but the credentials may be different.

Crosswork Hierarchical Controller sends SYSLOG events when the:

- Adapter fails to parse files
- Adapter fails to connect to the controller, for example, **Authentication failure** or **TCP Connection failed**.

Adapter Status Values

The following statuses are available for the devices assigned to an adapter (and as a total for all the devices assigned to the adapter) in the **Adapters** table in Device Manager.

	Information Types		
Possible values	**Inventory**	**Topology**	**Statistics**
OK	When the adapter collecting the specific info type successfully reached the device NMS system or device itself and discovered the device data.		
ERROR	When the adapter collecting the info type reached the device but could not collect the required information, for example, wrong credentials, command type error, or no data.		
UNREACHABLE	When the adapter collecting the info type failed to reach the device, typically as a result of a problem with connectivity.		

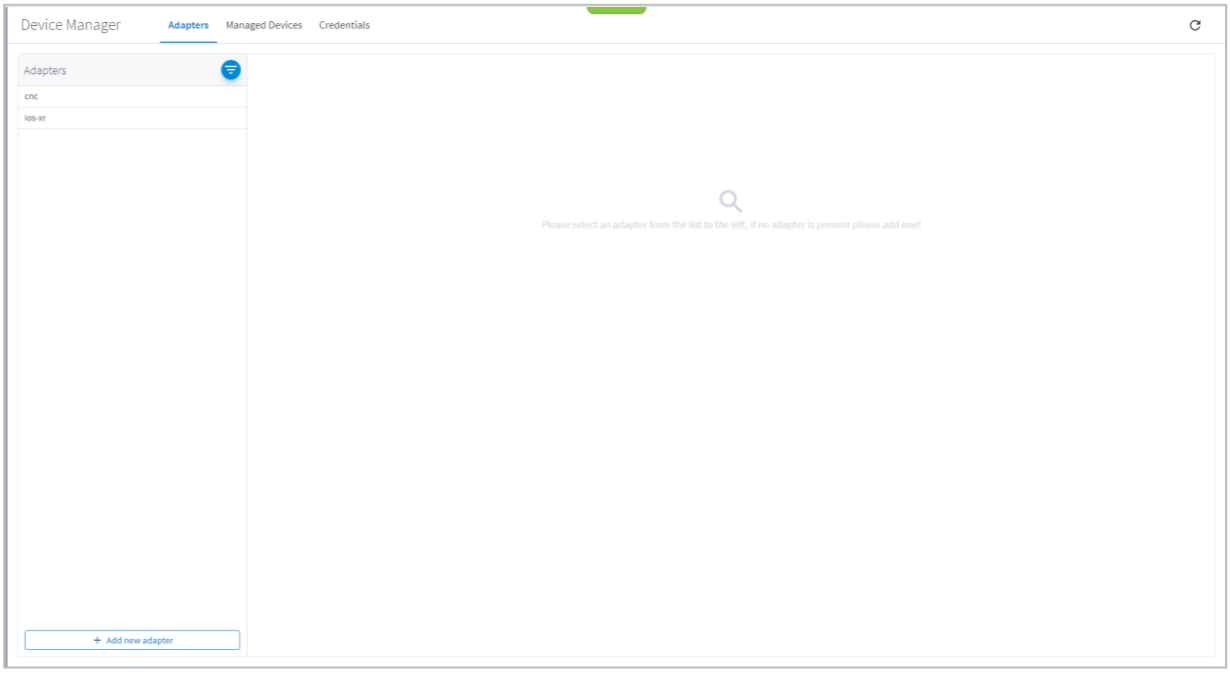
	Information Types		
Possible values	**Inventory**	**Topology**	**Statistics**
WARNING	N/A	N/A	When the adapter that collects statistics failed to get the data of some device ports.
UNKNOWN	When no status was reported by the adapter. This occurs when there is an internal communication error. Refer this to support.		

View Adapters

You can view a list of the adapters and see a list of the devices assigned to each adapter and the device status for inventory, topology, and statistics, as well as the events raised by the adapter.

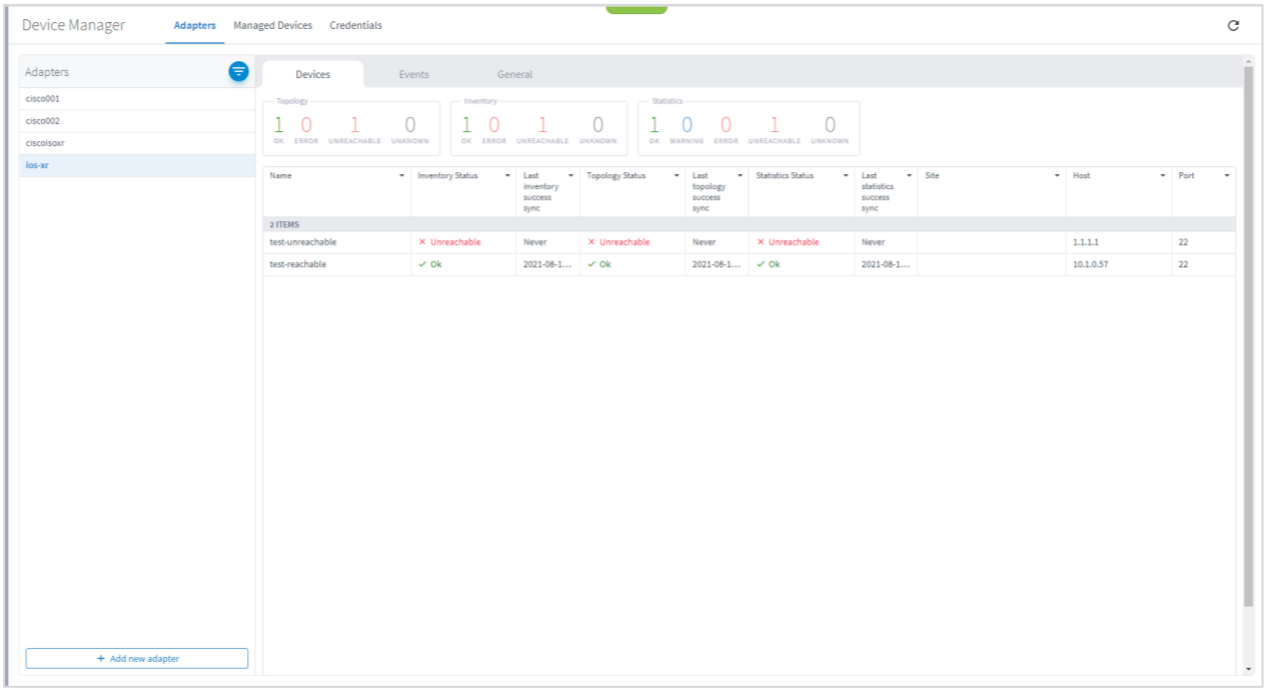
To view adapters:

1. In the applications bar, select **Services > Device Manager > Adapters**. A list of the adapters appears in the **Adapters** pane.

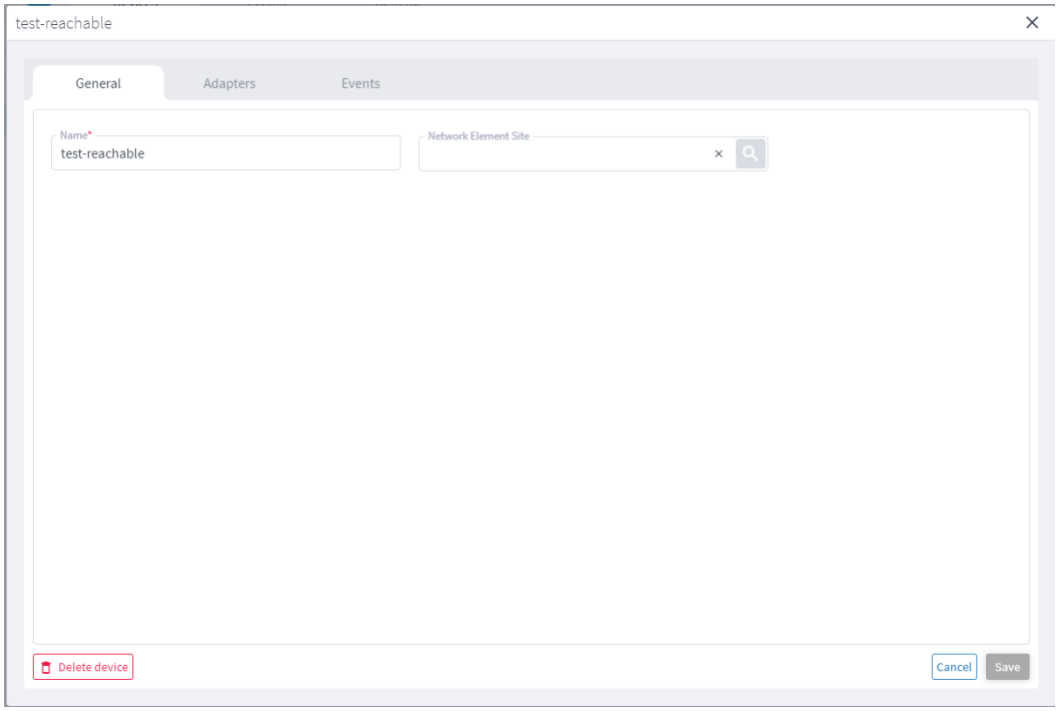


2. Select the required adapter. A summary of how many devices are **OK, ERROR, UNREACHABLE** or **UNKNOWN** for **Topology, Inventory** and **Statistics** appear, as well as a list of the assigned devices with the following information per device:
   - **Name**
   - **Topology Status**
   - **Last topology success sync**
   - **Inventory Status**
   - **Last inventory success sync**

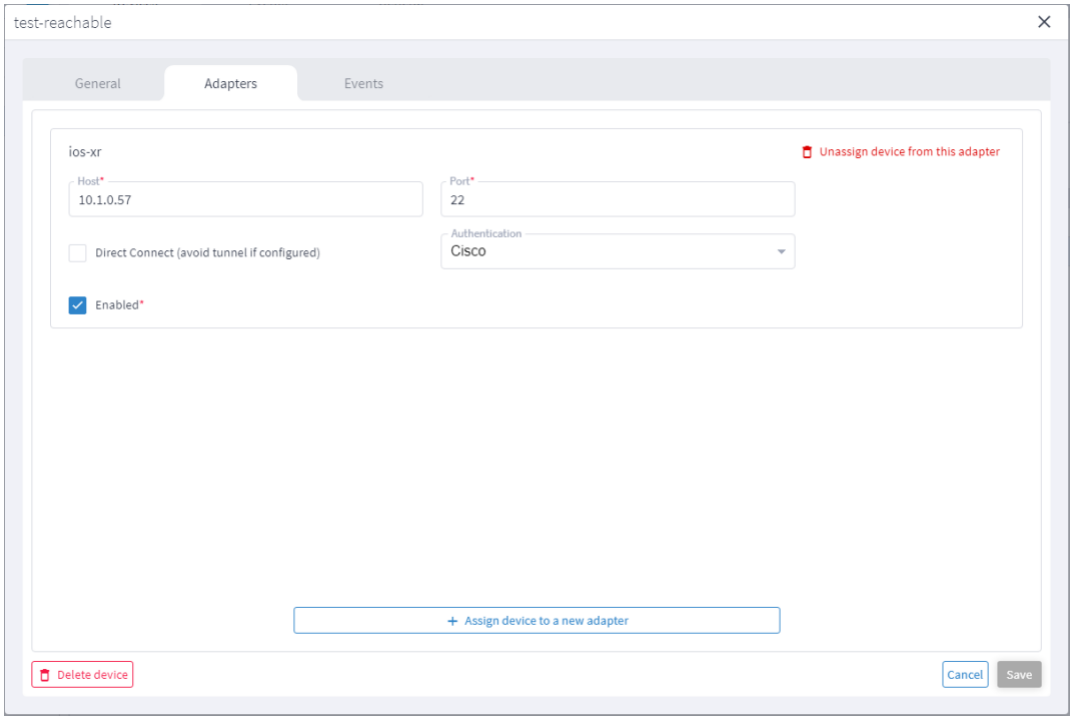
- **Statistics Status**
- **Last statistics success sync**
- **Site**
- **Host**
- **Port**



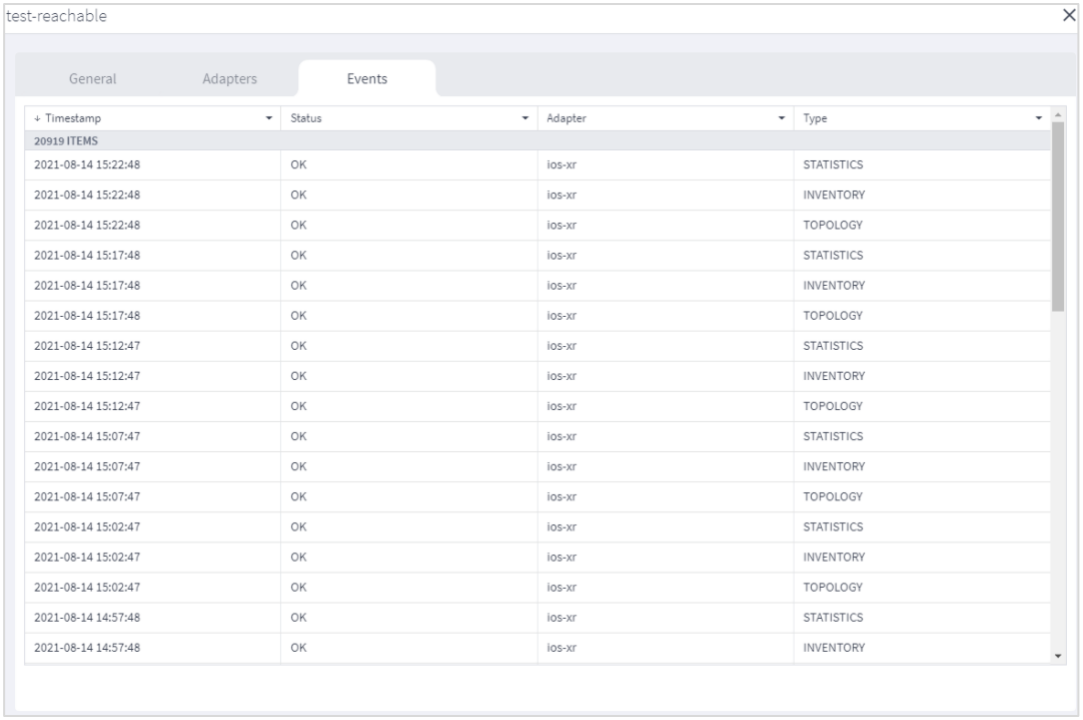
3. Hover over a device name to view the device in the map and click **Open in Explorer** to open the device in Explorer (or click on the device directly to view the device in Explorer).
4. To view the device details, click on any of the columns (except the **Name** column).



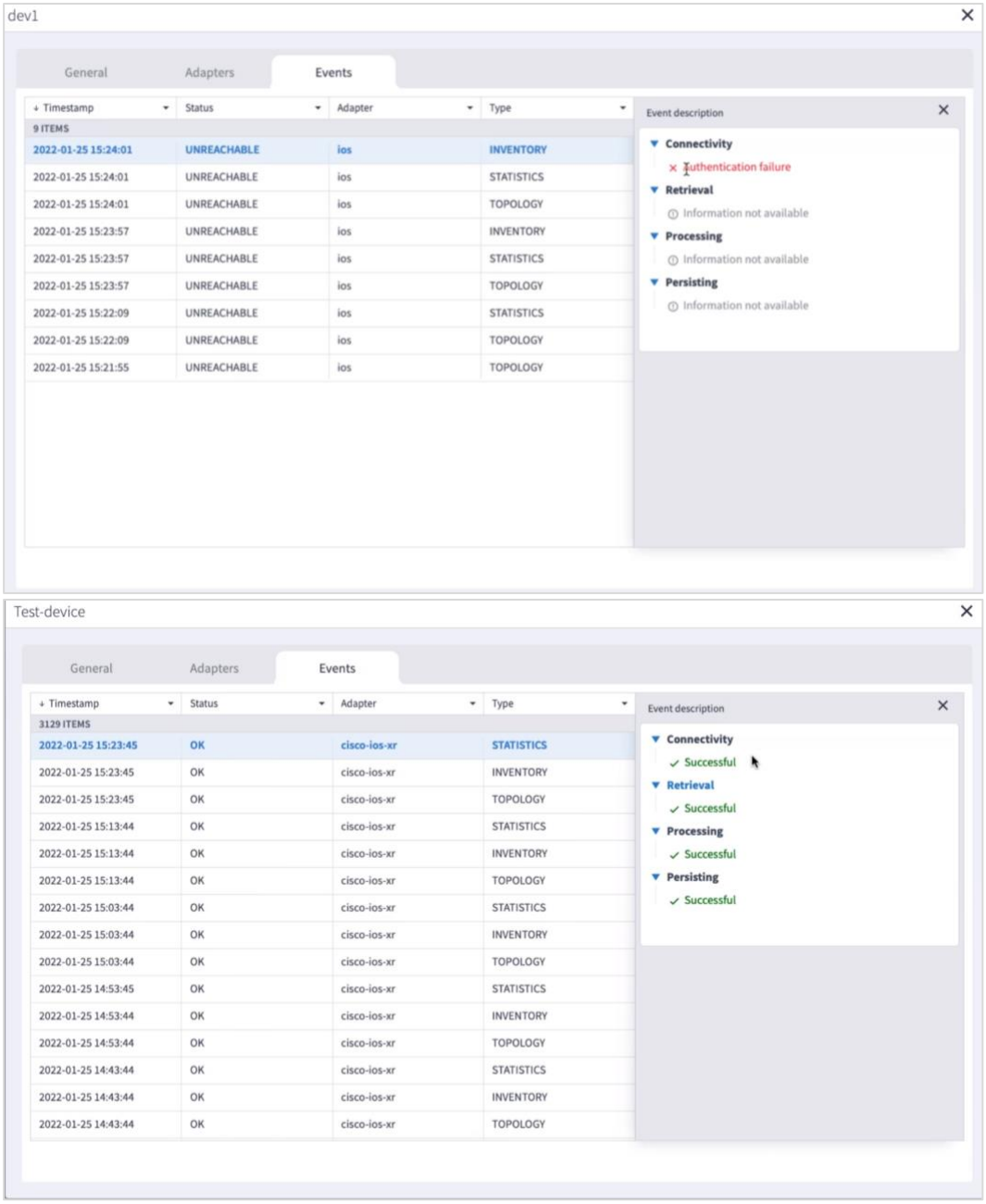
5. To view the device adapters, select the **Adapters** tab.



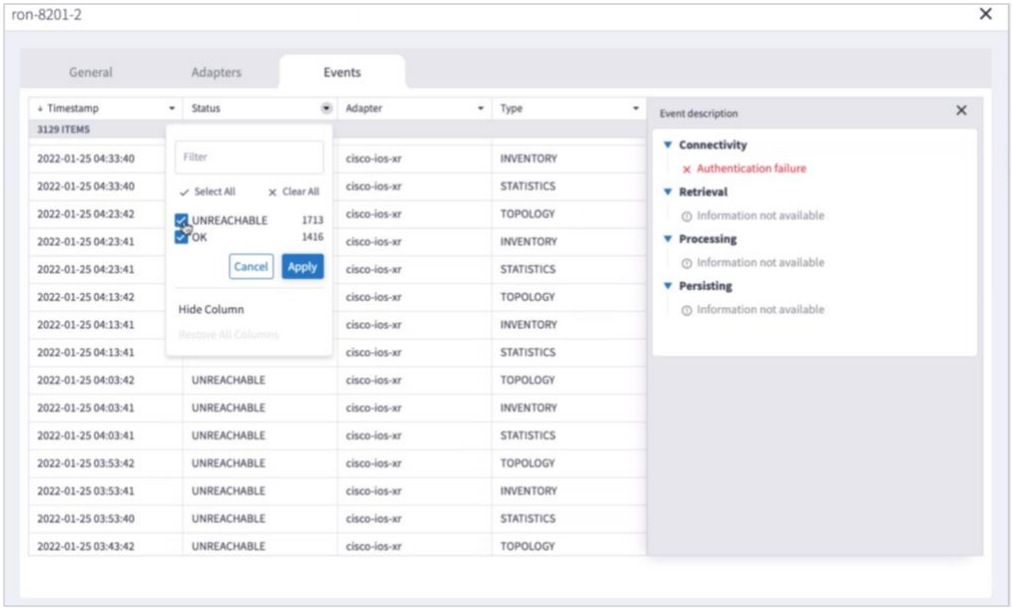
6. To view the device events, select the **Events** tab.



7. To view further details, click on an event.



8. Click to filter by event **Status**.



Edit Device

You can edit a device and select the network element in Explorer, assign the device to an adapter or unassign the device from an adapter.

To edit a device:

1. In the applications bar in Crosswork Hierarchical Controller, select **Services > Device Manager**.
2. Select the required adapter.
3. Select the **Managed Devices** tab.
4. Click on the required device row (not on the link in the **Name** column).
5. In the **General** tab, in **Network Element** Site click to select the network element in Explorer.

Edit Adapter

You can edit the adapter configuration and enable or disable the adapter, set the logging level and polling cycle, specify the number of concurrent routers to poll in each polling cycle, and select the required collection parameters. You can also edit any adapter-specific parameters. To add or remove devices from an adapter, see Managed Devices.

To edit adapters:

1. In the applications bar in Crosswork Hierarchical Controller, select **Services > Device Manager**. A list of the adapters appears in the **Adapters** pane.
2. Select the required adapter.
3. Click the **General** tab.
4. Configure the following options:
   - **Enabled**: Whether the adapter is enabled or disabled.
   - **Logging Level**: The logging level (Info, Critical, Error, Warning, Debug). Info by default.

- **Polling Cycle (sec)**: The polling interval in seconds.
- **Number of concurrent routers collected**: The number of network elements that can be concurrently polled in a polling cycle.
- **Enable provisioning support**: Whether to enable provisioning support. For example, if provisioning is enabled, creating a new tunnel or service.

5. Configure the **SSH CONFIGURATION PARAMETERS** (for adapters that are configured to work with SSH):
   - **Enable Tunnel:** This enables the tunnel.
   - **Tunnel Host:** The tunnel host.
   - **Tunnel Port:** The tunnel port.
   - **Tunnel Credentials Key:** The tunnel
   - **Router Connect timeout:** The router connect timeout.
   - **Router Command timeout:** The router command timeout.
6. Configure the **FILE BRINGER PARAMETERS**:
   - **Enable File Bringer**: This enables the module in the adapter to transfer the files from the remote file server to Crosswork Hierarchical Controller.
   - **File Server Location**: The file server location In the format *http/sftp:///<ip>:port/<path>*.
   - **File Type**: For example, CSV, JSON.
   - **Authentication**
   - **Backup File Server Location**: The backup file server location In the format *http/sftp:///<ip>:port/<path>*.
   - **Backup_server_authentication**
7. Configure the **NETFUSION COLLECTION CYCLES FILES**:
   - **Enable NetFusion Cycles mode**: Whether to get the files periodically or not.
   - **Cycle Directories Location**: Where to store the files received in Crosswork Hierarchical Controller.
8. Configure any other adapter-specific parameters, if any.
9. Configure the **COLLECTION PARAMETERS** (common to all IP adapters):
   - **Enable Topology Collection**
   - **Enable IGP IS-IS Collection**
   - **Enable IGP OSPF Collection**
   - **Enable Interface Stats Collection**
   - **Enable VRF Collection**
   - **Enable LLDP Collection**
   - **Enable MLPS Tunnels Collection**
   - **Enable LSP Stats Collection**

- **Enable SNMP Collection**
- **IGP IS-IS Priority**
- **Collect only IGP IS-IS seed routers**
- **Allow to use loopback IP as management IP**
- **Enable RSVP Collection**
- **Enable collection of optics and coherent DSP**
- **Enable Segment Routing Collection**

10. Click **Save**.

Add Adapter

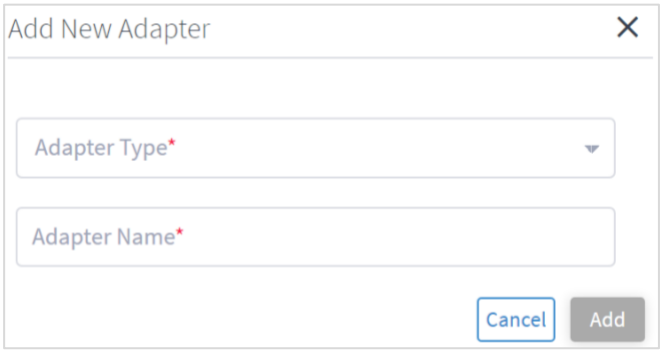
An adapter is an instance of an adapter type. The adapter types are usually pre-installed with Crosswork Hierarchical Controller (adapter types can also be added without impacting the Crosswork Hierarchical Controller platform installation).

You can also configure any adapter-specific parameters (these are added per project).

To add or remove devices from an adapter, see Managed Devices.

To add an adapter:

1. In the applications bar in Crosswork Hierarchical Controller, select **Services > Device Manager**. A list of the adapters appears in the **Adapters** pane.
2. Click **Add new adapter**.



3. Enter the adapter details:
   - **Adapter Type**: Select an adapter type from the list of available adapter types currently installed in Crosswork Hierarchical Controller.
   - **Adapter Name**: Unique user defined name of this adapter type instance (there can be several instances of the same adapter type).
4. Click **Add**.
5. To configure the adapter, select the adapter in the **Adapters** pane.
6. Click the **General** tab.
7. Configure the following options:
   - **Enabled**: Whether the adapter is enabled or disabled.

- **Logging Level**: The logging level (**Info**, **Critical**, **Error**, **Warning**, **Debug**). **Info** by default.
- **Polling Cycle (sec)**: The polling interval in seconds.
- **Number of concurrent routers collected**: The number of network elements that can be concurrently polled in a polling cycle.
- **Enable provisioning support**: Whether or not to enable provisioning support. For example, if provisioning is enabled, creating a new tunnel or service.

8. Configure the **SSH CONFIGURATION PARAMETERS** (for adapters that are configured to work with SSH):
   - **Enable Tunnel**
   - **Tunnel Host**
   - **Tunnel Port**
   - **Tunnel Credentials Key**
   - **Router Connect timeout**
   - **Router Command timeout**
9. Configure the **FILE BRINGER PARAMETERS**:
   - **Enable File Bringer**: This enables the module in the adapter to transfer the files from the remote file server to Crosswork Hierarchical Controller.
   - **File Server Location**: The file server location In the format **http/sftp://<ip>:port/<path>**.
   - **File Type**: For example, CSV, JSON.
   - **Authentication**
10. Configure the **NETFUSION COLLECTION CYCLES FILES**:
    - **Enable NetFusion Cycles mode**: Whether to get the files periodically or not.
    - **Cycle Directories Location**: Where to store the files received in Crosswork Hierarchical Controller.
11. Configure any other adapter-specific parameters, if any.
12. Configure the **COLLECTION PARAMETERS** (common to all IP adapters):
    - **Enable Topology Collection**
    - **Enable IGP IS-IS Collection**
    - **Enable IGP OSPF Collection**
    - **Enable Interface Stats Collection**
    - **Enable VRF Collection**
    - **Enable LLDP Collection**
    - **Enable MLPS Tunnels Collection**
    - **Enable LSP Stats Colleciton**
    - **Enable SNMP Collection**

- **IGP IS-IS Priority**
- **Collect only IGP IS-IS seed routers**
- **Allow to use loopback IP as management IP**
- **Enable RSVP Collection**
- **Enable collection of optics and coherent DSP**
- **Enable Segment Routing Collection**

13. Click **Save**.
14. Assign devices to the adapter. See Assign Device.

Delete Adapter

To delete an adapter:

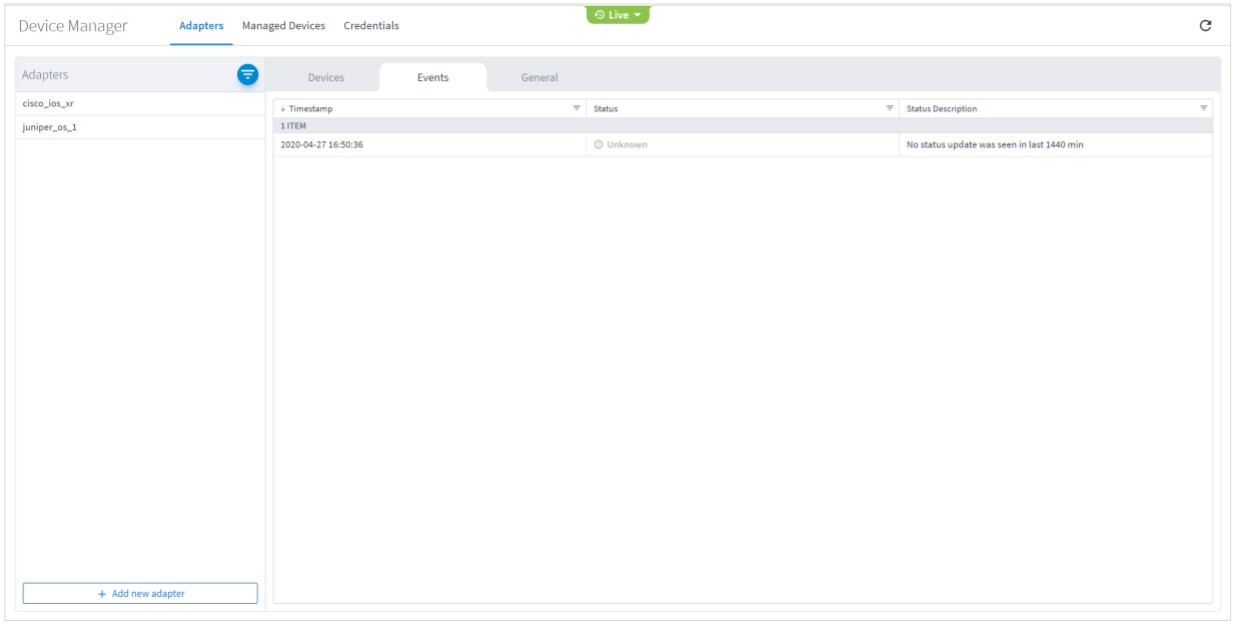
1. In the applications bar in Crosswork Hierarchical Controller, select **Services > Device Manager**. A list of the adapters appears in the Adapters pane.
2. Select an adapter.
3. Select the **General** tab.
4. Click **Delete Adapter**. A confirmation message appears.
5. Click **Confirm**. The adapter is deleted.

View Adapter Events

You can view the user-driven and system-driven events for a specific adapter. The adapter events vary according to the adapter type.

To view adapter events:

1. In the applications bar in Crosswork Hierarchical Controller, select **Services > Device Manager**. A list of the adapters appears in the **Adapters** pane.
2. Click to select the required adapter.
3. Select the **Events** tab**.**



4. The event table details:
    - Timestamp
    - Status
    - Status Description

Managed Devices

The following statuses are available per device (and as a total for all the devices) in the **Managed Devices** table in Device Manager.

	Information Types		
Possible values	**Inventory**	**Topology**	**Statistics**
OK	When the adapter collecting the specific info type successfully reached the device NMS system or device itself and discovered the device data.		
ERROR	When the adapter collecting the info type reached the device but could not collect the required information, for example, wrong credentials, command type error, or no data.		
UNREACHABLE	When the adapter collecting the info type failed to reach the device, typically as a result of a problem with connectivity.		
WARNING	N/A	N/A	When the adapter that collects statistics failed to get the data of some device ports.
UNKNOWN	When no status was reported by the adapter. This occurs when there is an internal communication error. Refer this to support.		

Crosswork Hierarchical Controller sends SYSLOG events when the device reachability state changes.

You can add devices and assign them to adapters.

Add Device and Assign to Adapters

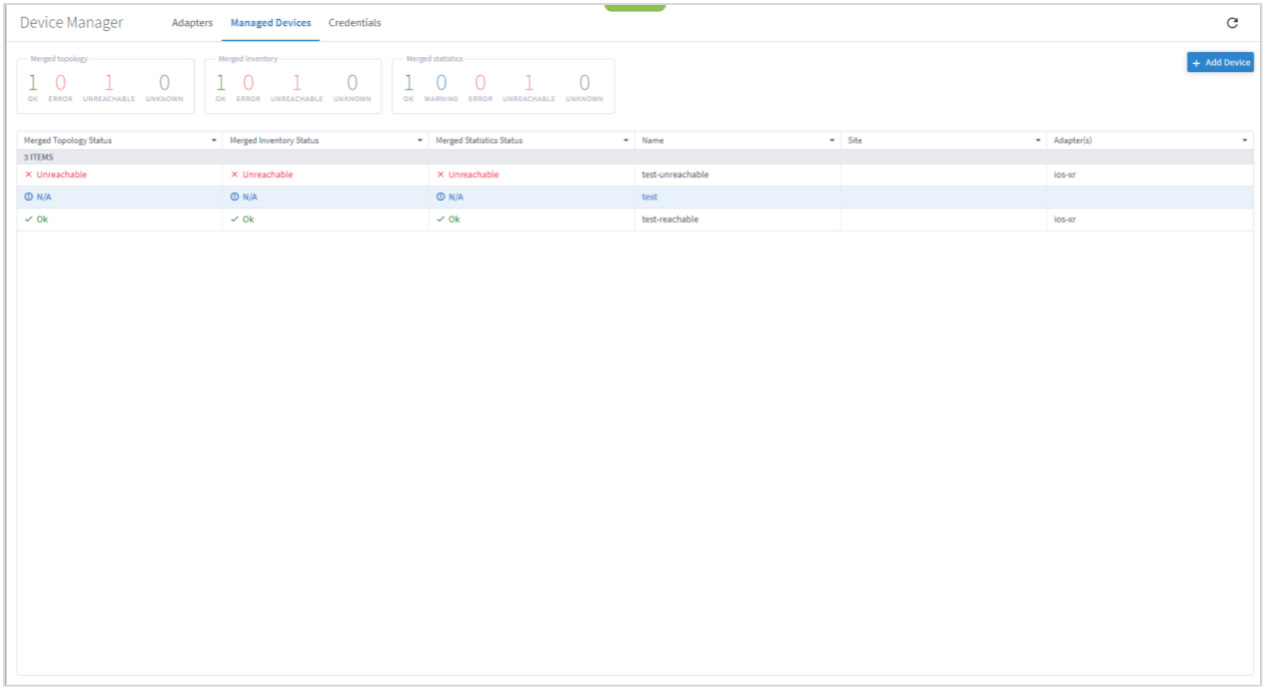
You can add a device, and then assign it to one or more adapters.

Ensure that you have added the required credential before assigning the device to an adapter. See Credentials.

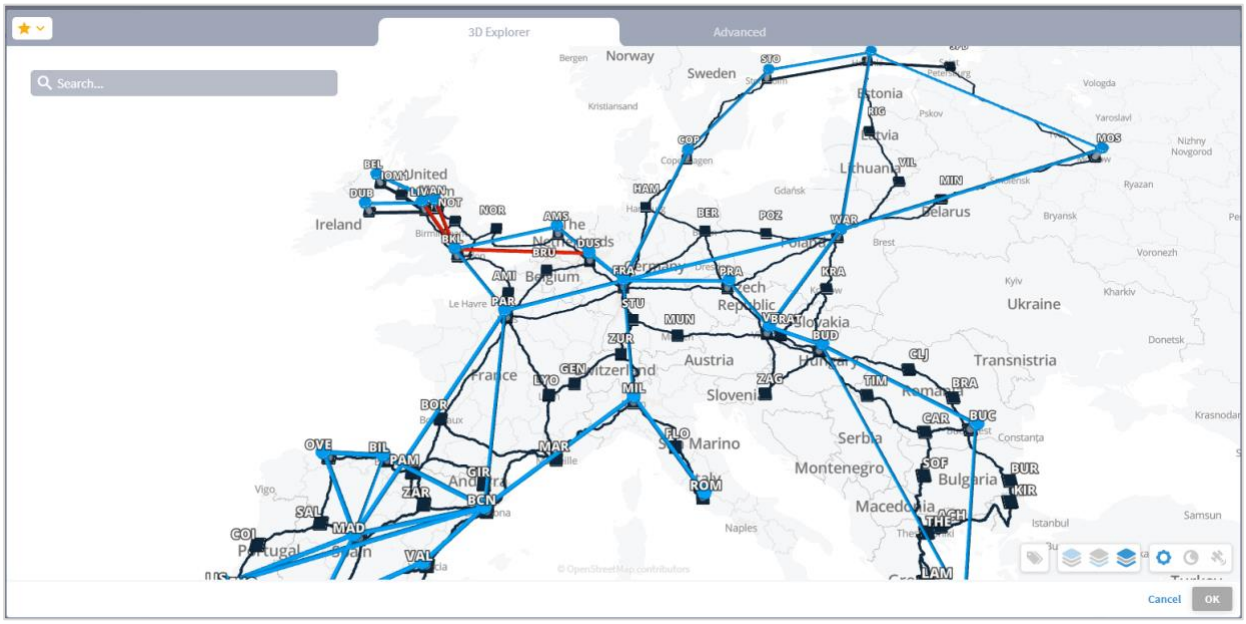
To add a device:

1. In the applications bar in Crosswork Hierarchical Controller, select **Services > Device Manager**. A list of the adapters appears in the **Adapters** pane.

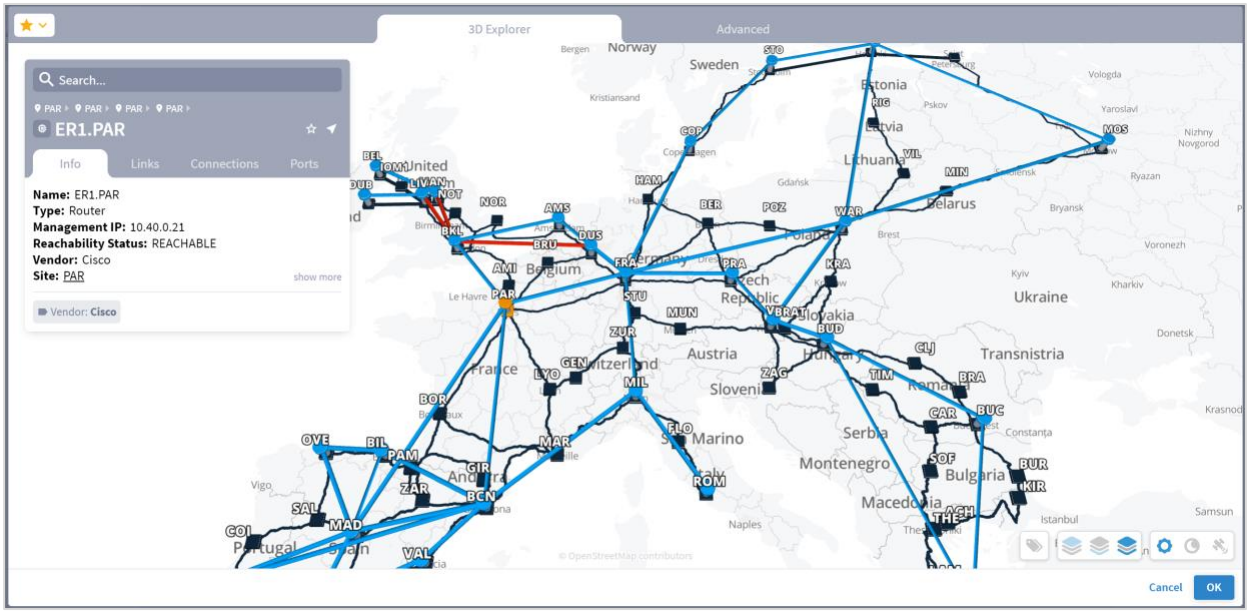
2. Select the **Managed Devices** tab.



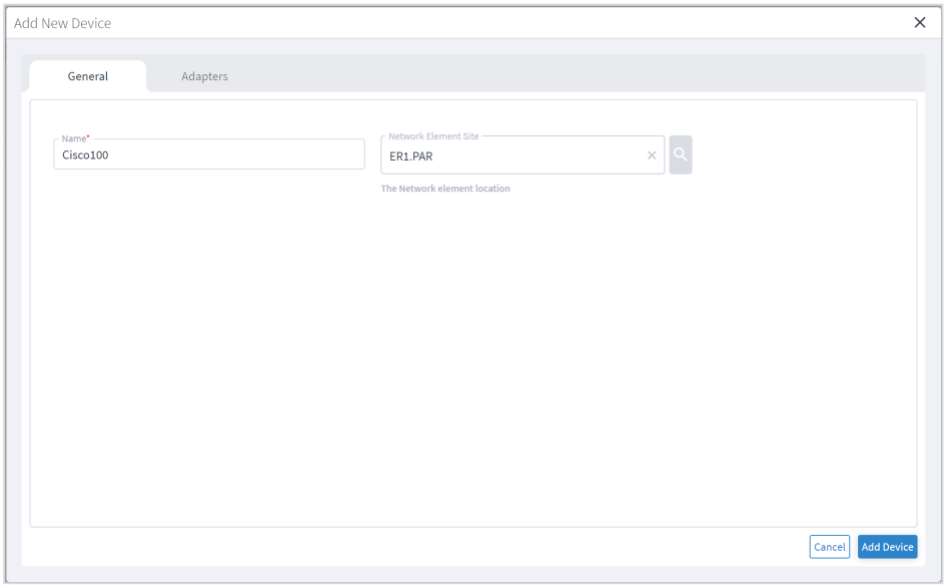
3. Click **Add Device**.
4. In the General tab, enter the **Name.**
5. (Optional) In **Network Element Site** click to select a site where the device is located.



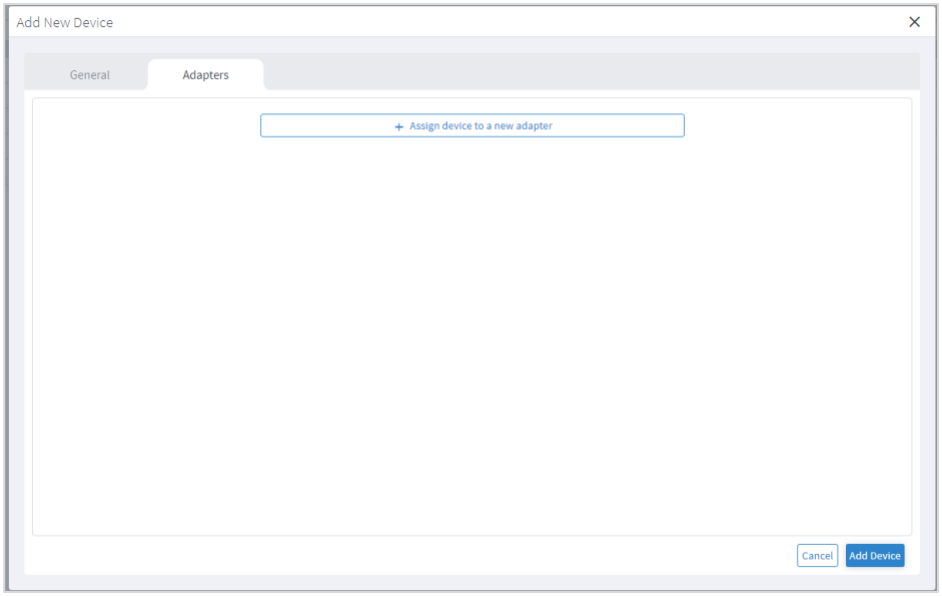
6. Select the network element.



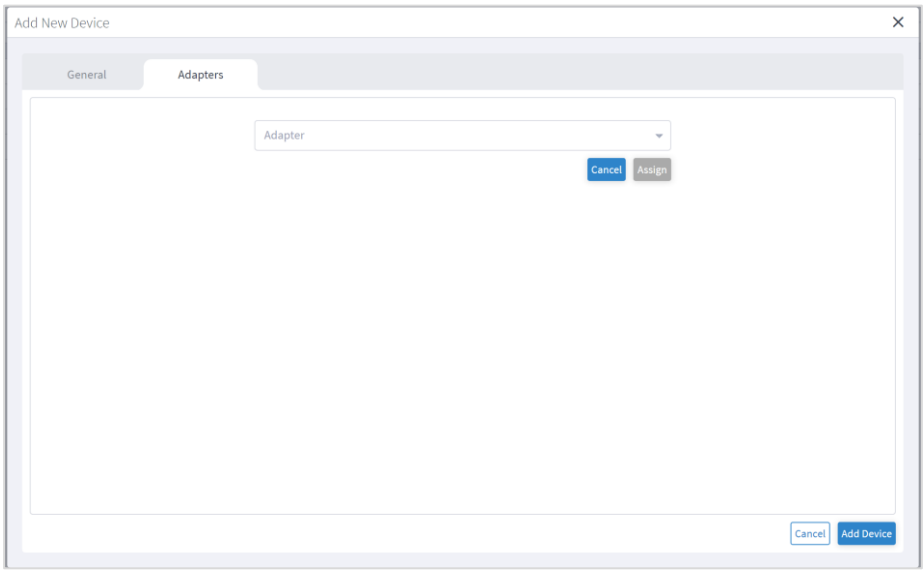
7. Click **OK**.



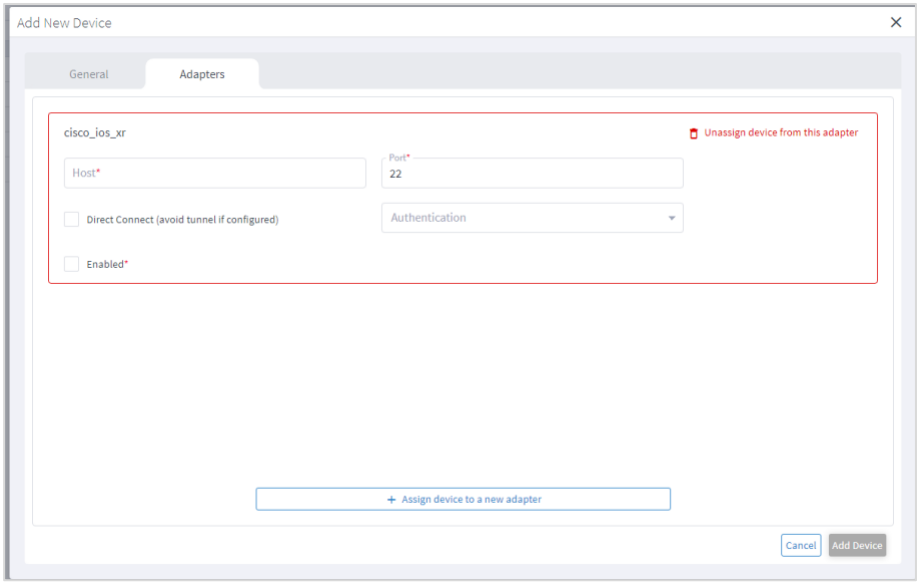
8. Select the **Adapters** tab.



9. Click **Assign device to a new adapter**.



10. Select the adapter to assign the device to and click **Assign**.



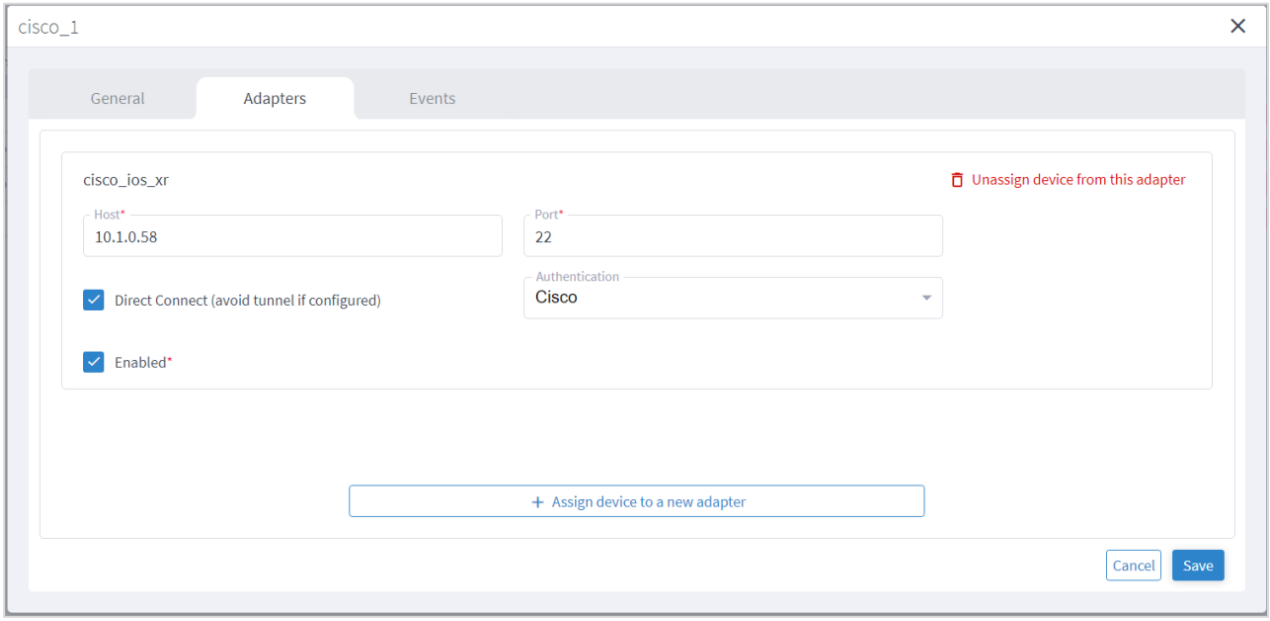
11. Complete the details for the adapter:
    - **Host**
    - **Port**
    - **Direct Connect** (avoid tunnel if configured)
    - **Authentication** (this is the credential)
    - **Enabled**
12. Click **Save**.
13. Repeat for as many adapters as required.
14. Click **Add Device**.

Assign Device to an Adapter

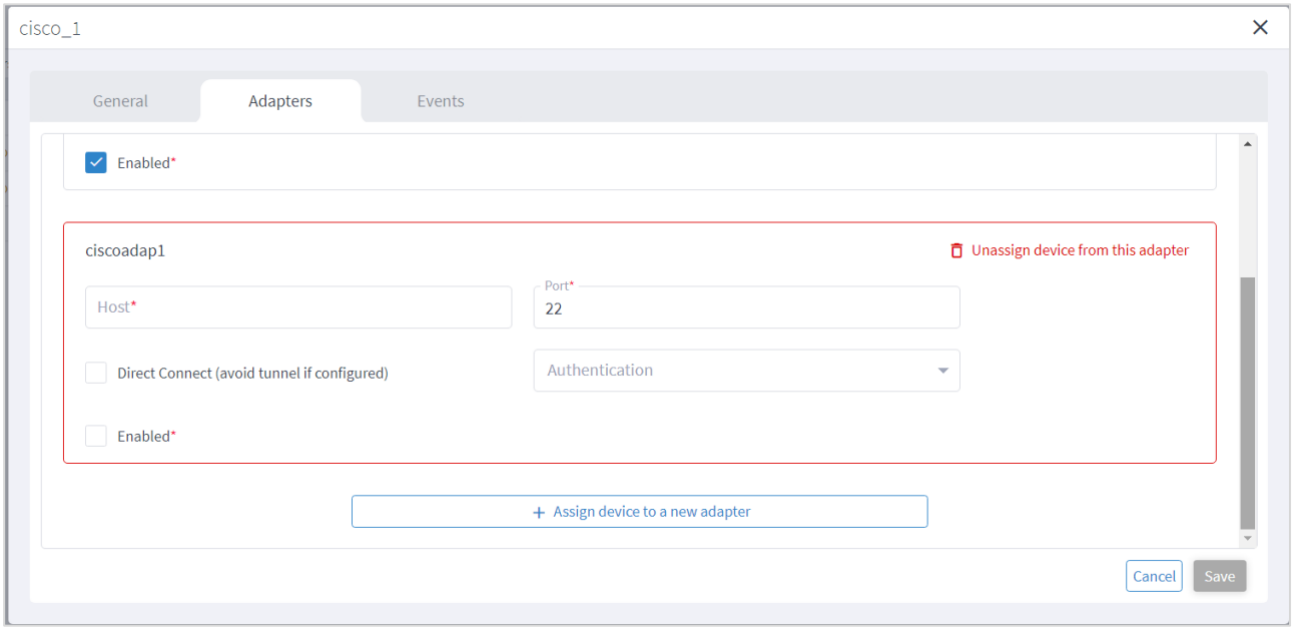
You can assign a device to one or more adapters.

To assign a device:

1. In the applications bar in Crosswork Hierarchical Controller, select **Services > Device Manager**.
2. Select the **Managed Devices** tab.
3. Click on the required device row (not on the link in the **Name** column).
4. Select the **Adapters** tab.



5. Click **Assign device to a new adapter**.
6. Select an **Adapter** and click **Assign**.



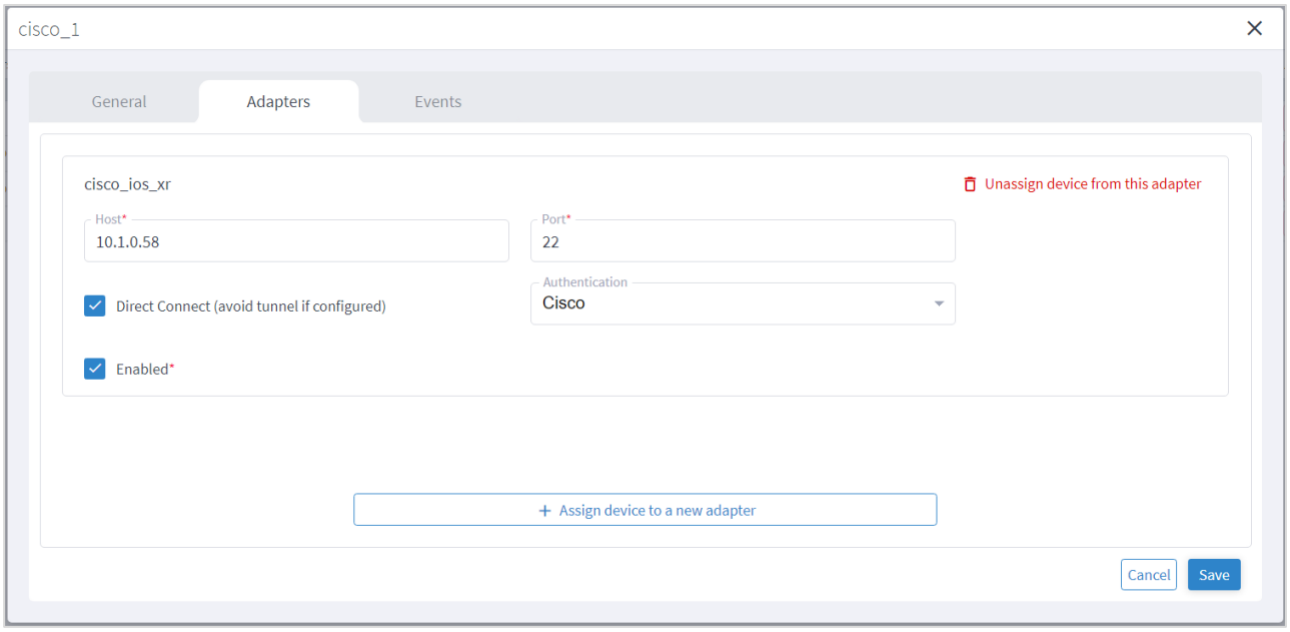
7. Complete the following:
    - **Host**
    - **Port**
    - **Direct Connect** (avoid tunnel if configured)
    - **Authentication** (this is the credential)
    - **Enabled**
8. Click **Save**.

Unassign Device

You can unassign a device from an adapter. The device is removed from the adapter but remains in the model.

To unassign a device from an adapter (from the device):

1. In the applications bar in Crosswork Hierarchical Controller, select **Services > Device Manager**.
2. Select the **Managed Devices** tab.
3. Click on the required device row (not on the link in the **Name** column).
4. Select the **Adapters** tab.



5. Click **Unassign device from this adapter**.
6. Click **Save**.

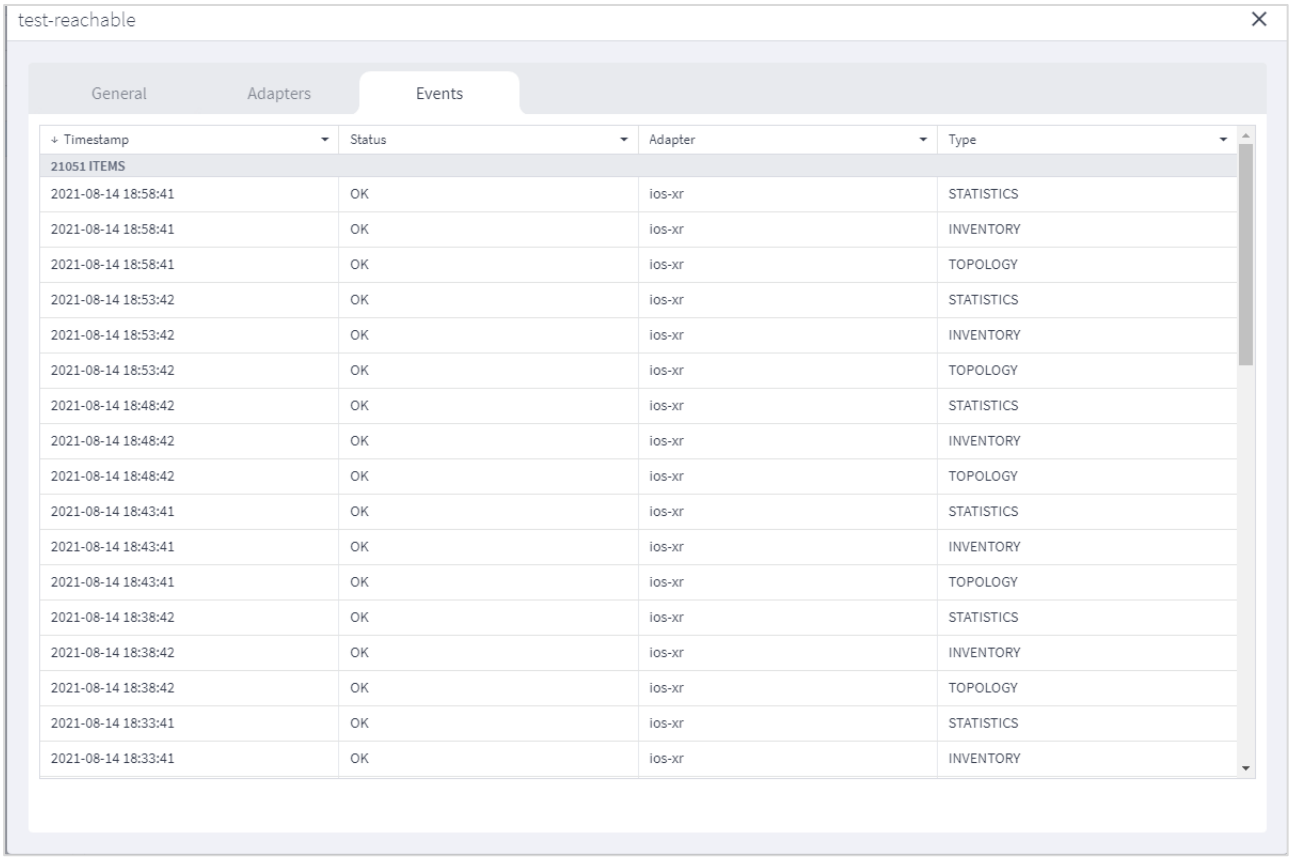
View Device Events

You can view the events for a device. The adapters poll the devices periodically.

To view device events:

1. In the applications bar in Crosswork Hierarchical Controller, select **Services > Device Manager**.
2. Select the **Managed Devices** tab.

3. Click on the required device row (not on the link in the **Name** column).
4. Select the **Events** tab.



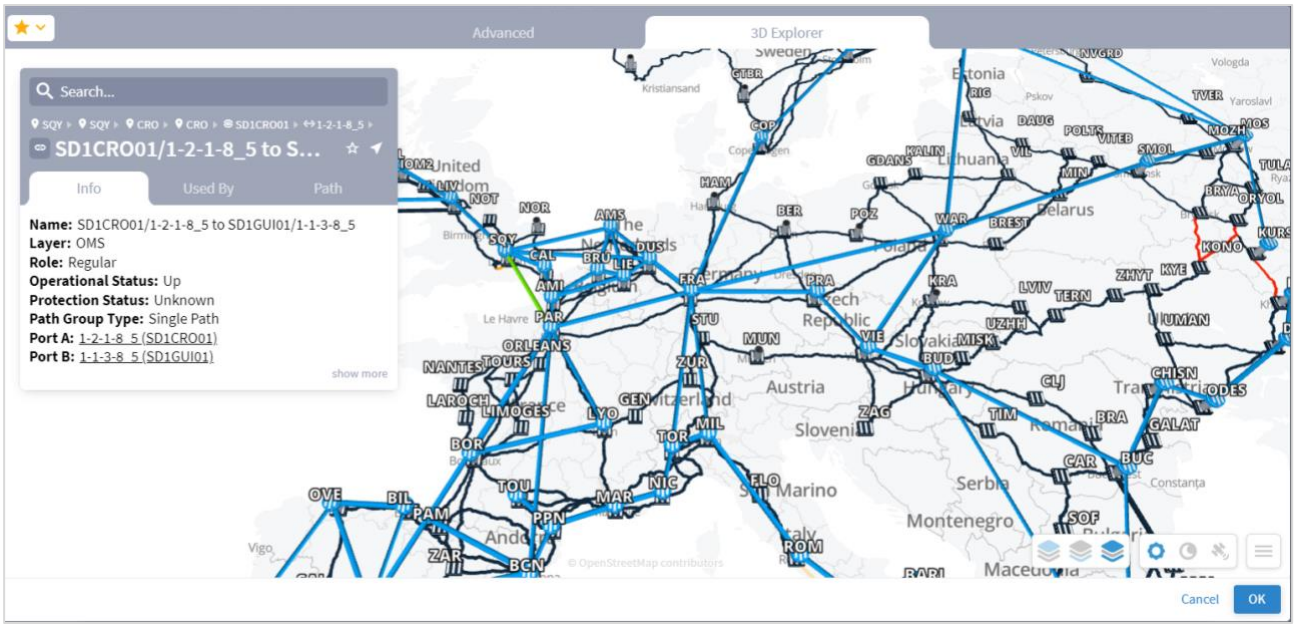
Edit Device

You can edit a device and select the network element in Explorer, assign the device to an adapter or unassign the device from an adapter.

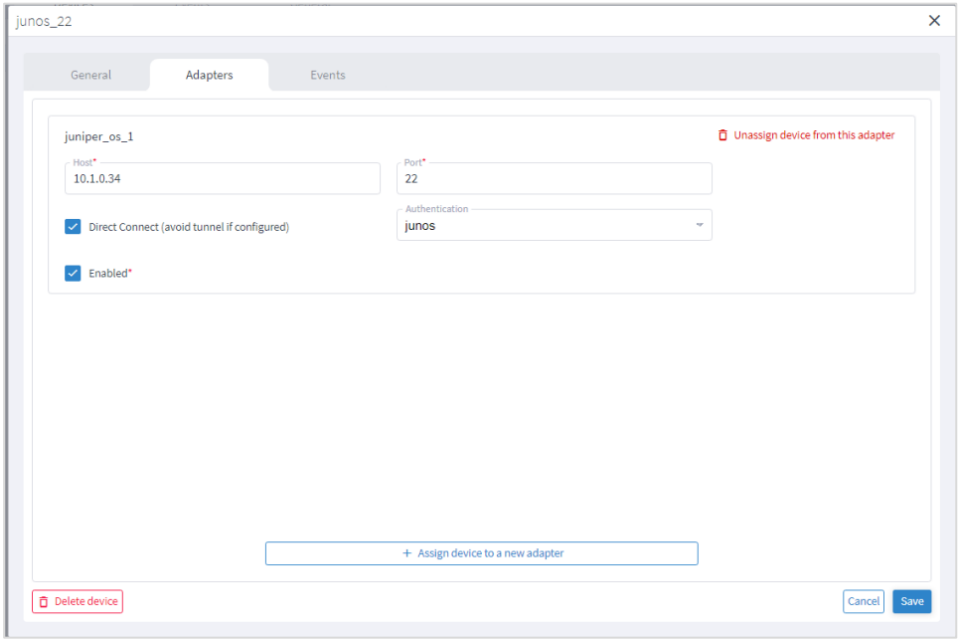
To edit a device:

1. In the applications bar in Crosswork Hierarchical Controller, select **Services > Device Manager**.
2. Select the required adapter.
3. Select the **Managed Devices** tab.
4. Click on the required device row (not on the link in the **Name** column).
5. In the **General** tab, in **Network Element Site** click to select the network element in Explorer.

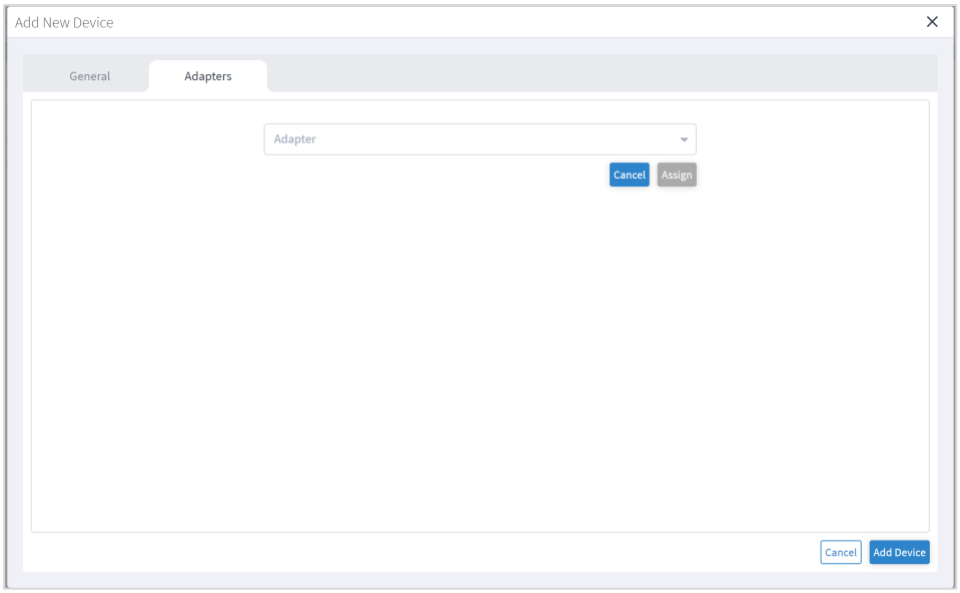
6. Select the **3D Explorer** tab.
7. Select the network element.



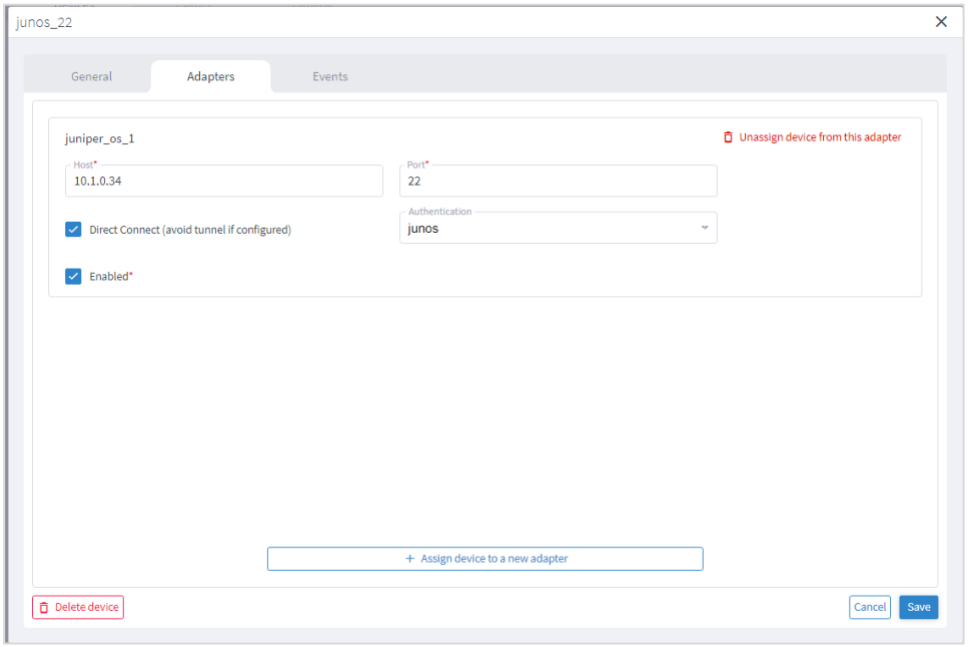
8. Click **OK**.
9. Select the **Adapters** tab.



10. To unassign the device from an adapter, click **Unassign device from the adapter**.
11. To assign the device to an adapter, click **Assign device to a new adapter**.



12. Select the adapter to assign the device to and click **Assign**.



13. Complete the details for the adapter:
    - **Host**
    - **Port**
    - **Direct Connect** (avoid tunnel if configured)
    - **Authentication** (this is the credential)
    - **Enabled**

14. Click **Save**.

Delete Device

You can delete a device and unassign it from its adapters. The device is deleted from the model.

Alternatively, if you want to keep the device in the model, and only unassign the device, see Unassign Device.

To delete a device:

1. In the applications bar in Crosswork Hierarchical Controller, select **Services > Device Manager**.
2. Select the required adapter.
3. Select the **Managed Devices** tab.
4. Click on the required device row (not on the link in the **Name** column).
5. Click **Delete device**. A confirmation message appears.
6. Click **Confirm** to delete the device, unassign it from all adapters and delete the device from the model

Model Settings

The network model includes regions (the geographical areas where network sites are located) and sites (the logical groupings in the network) are defined in the model. In addition, resources can be tagged with a text label which then can be used to filter in various applications.

For more on regions and sites, see the *Cisco Crosswork Hierarchical Controller Network Visualization Guide*.

Regions

Regions are the geographical areas where network sites are located. The Model Settings application enables you to view and filter regions, delete regions, export regions, and import regions. Cisco will usually collaborate with you to set up the regions in your model.

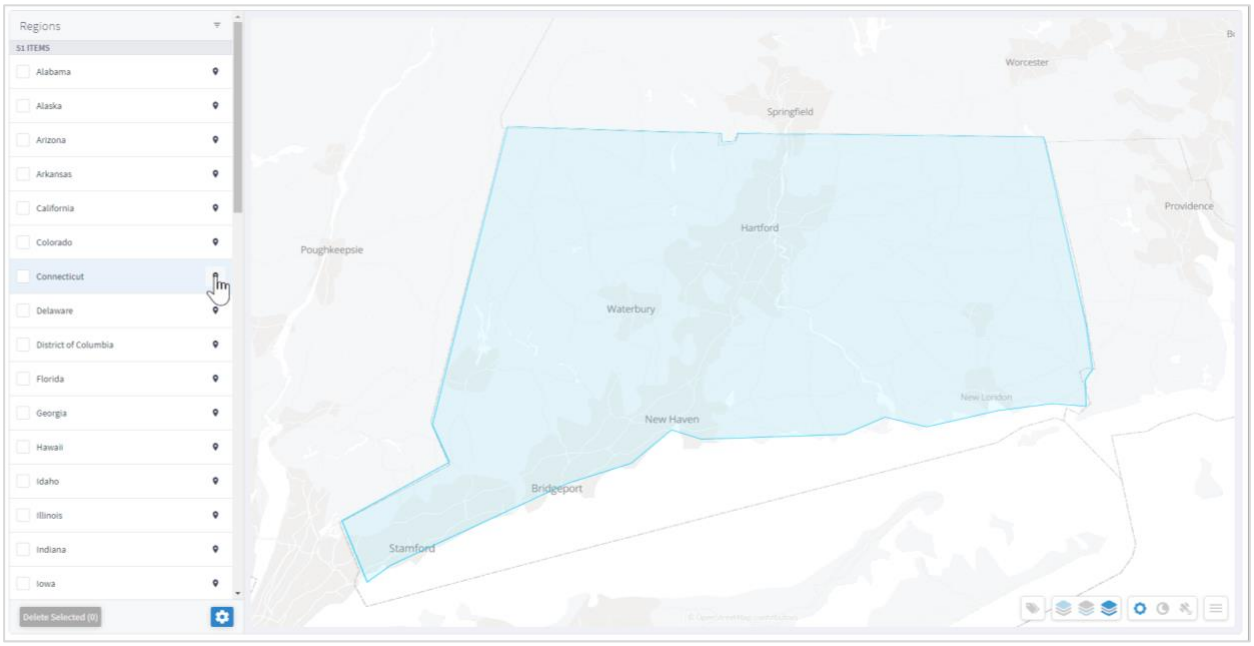
View a Region

You can view a region in **Model Settings**.

To view a region in Model Settings:

1. In the applications bar in Crosswork Hierarchical Controller, select **Services > Model Settings**.
2. Select the **Regions** tab.

3. To view a region, in **Regions**, click next to the required region, for example, **Connecticut**. The map moves to the selected region. The region is outlined.

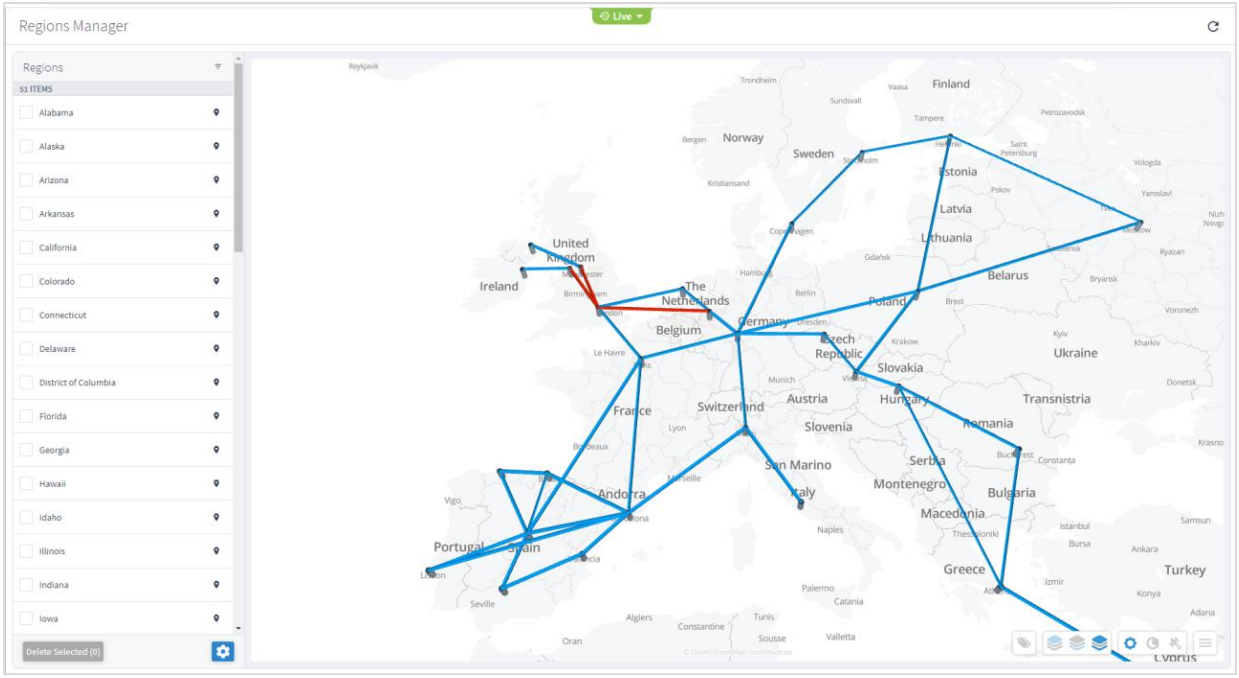


Filter the Regions

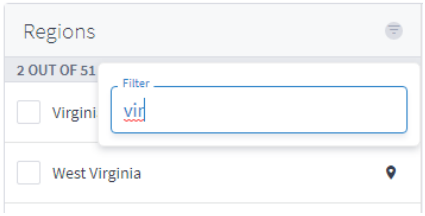
You can filter the regions.

To filter a region:

1. In the applications bar in Crosswork Hierarchical Controller, select **Services > Model Settings**.
2. Select the **Regions** tab.



3. To filter the regions, click and enter the filter criteria (case insensitive).

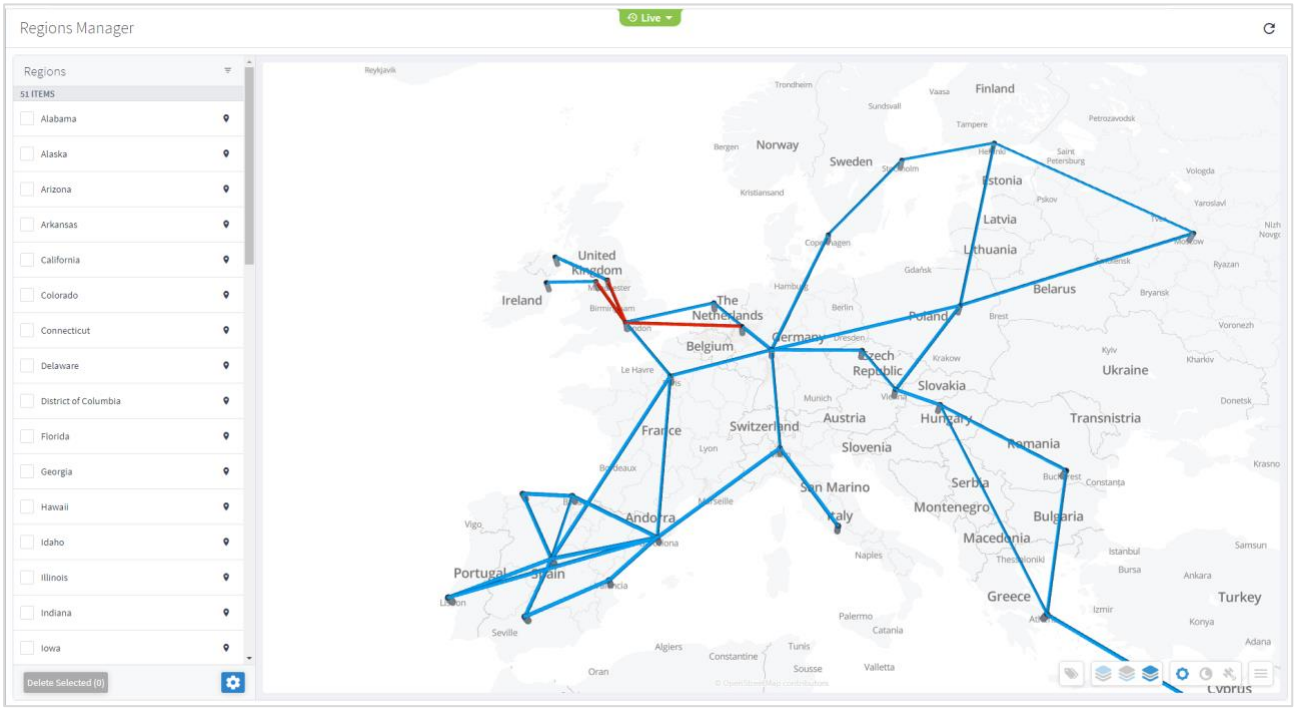


Delete Regions

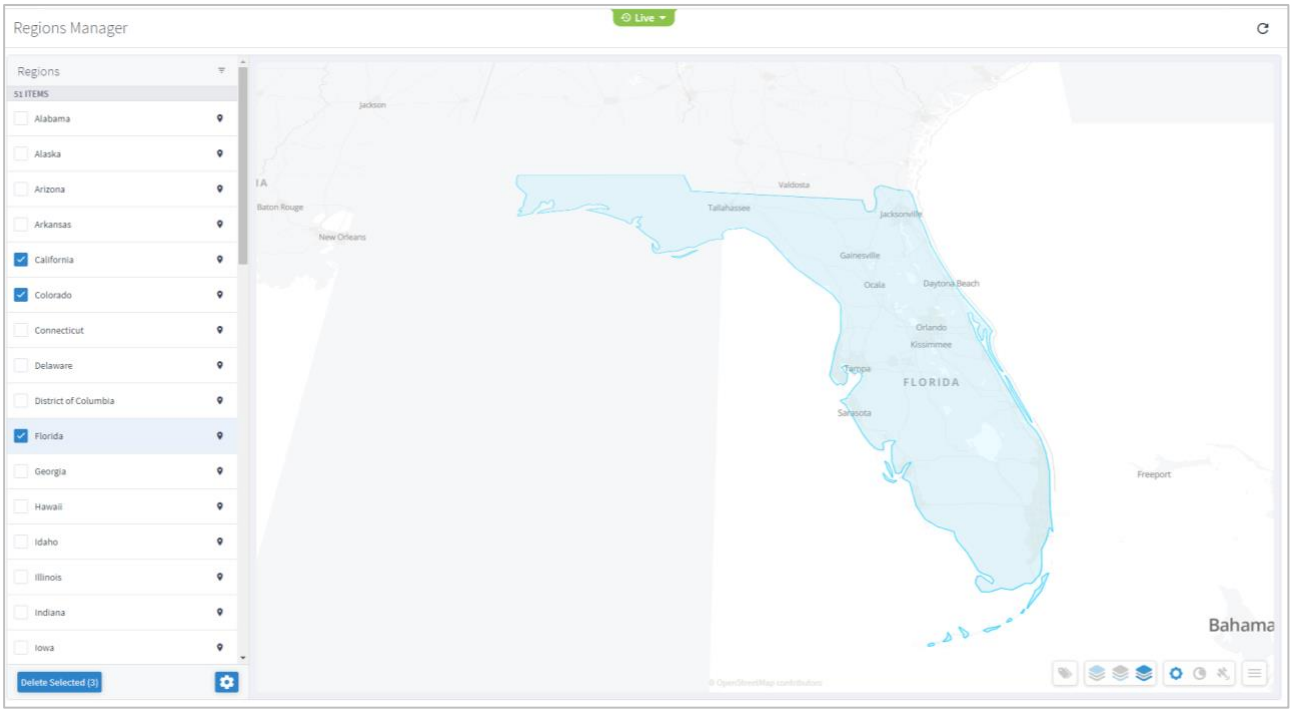
You can delete regions in Regions Manager.

To delete regions in Regions Manager:

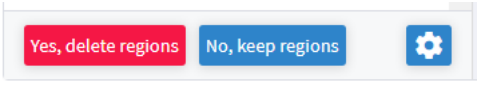
1. In the applications bar in Crosswork Hierarchical Controller, select **Services > Model Settings**.
2. Select the **Regions** tab.



3. In **Regions**, select one or more regions.



4. Click **Delete Selected**.



5. To delete the regions, click **Yes, delete regions**.

Export and Import Regions

Cisco will usually collaborate with you to set up the regions in your model. The regions are set up according to the standards published by http://geojson.io/ and can be exported or imported in GeoJSON or Region POJOs.

You can import (and export) regions in the following formats:

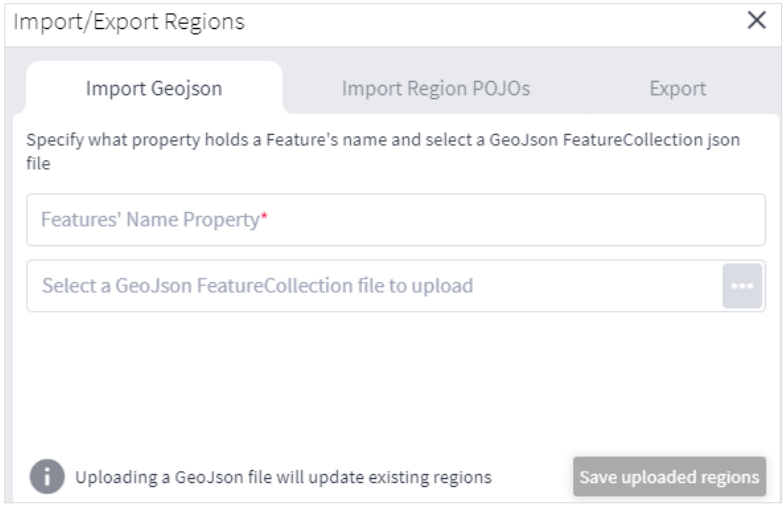
- GeoJSON
- Region POJOs

Valid geometry types for regions are:

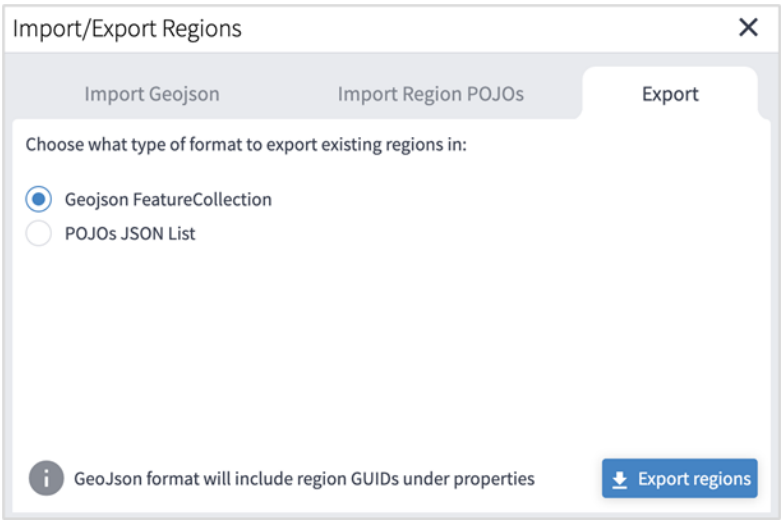
- Point
- LineString
- Polygon
- MultiPoint
- MultiLineString
- MultiPolygon

To export regions:

1. In the applications bar in Crosswork Hierarchical Controller, **select Services > Model Settings**.
2. Select the **Regions** tab.
3. In **Regions**, click .



4. To export In **Regions**, select the **Export** tab.

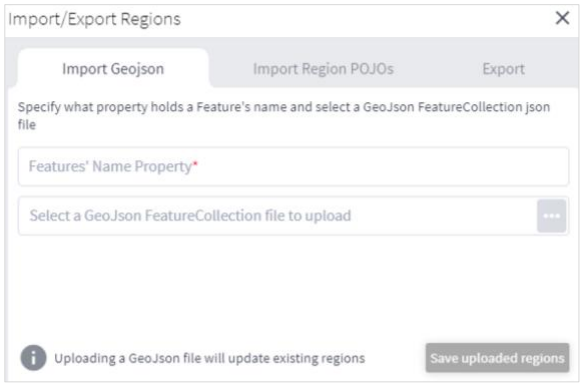


5. Select the required format, and then click **Export regions** . The JSON file is downloaded.
6. (Optional) Use a JSON formatter to review the content.

To import regions:

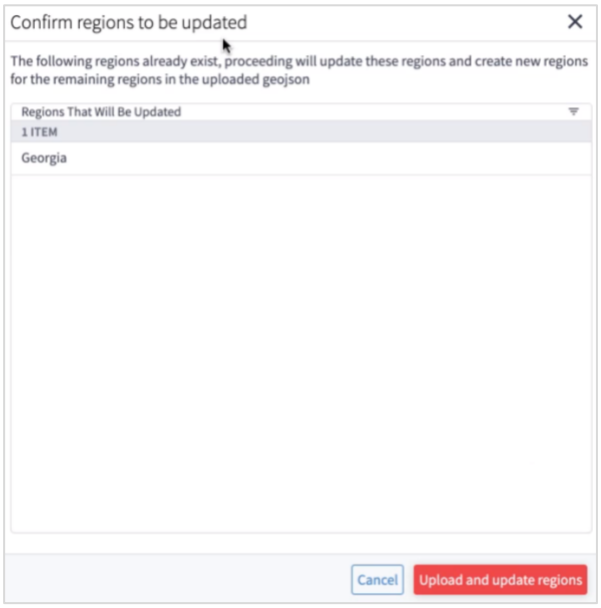
1. (Option 1) Prepare the import file in **GeoJSON** format:
   - A quick way to create the file in the correct format is to export the current regions in the required format and then edit the file.
   - The GeoJSON import file must be a **FeatureCollection** GeoJSON file and not a single **Feature** GeoJSON file.
   - The GeoJSON import file MUST have a region name property that will be specified when you import the file.
   - The GeoJSON import file may include a GUID for each region. If a GUID is not provided, Regions Manager, generates a GUID for the GeoJSON feature. If a GUID is provided, Regions Manager uses it, and if a region with that GUID already exists it is updated.
   - Each region name (and GUID if included) must only appear once.
   - Region names are case insensitive.
   - If a region already exists either by GUID or with an identical name, when you import the file, a message appears informing you that the region will be updated if you proceed.

2. (Option 2) Prepare the import file in Region POJOs format:
    - A quick way to create the file in the correct format is to export the current regions in the required format and then edit the file.
    - The RegionPOJO import file has a fixed format and the region name property is **name**. This property does not have to be specified when you import the file.
    - The RegionPOJO import file must include the region GUID as a property.
    - Each region name and GUID must only appear once.
    - Region names are case insensitive.
    - If a region already exists (by name or GUID), when you import the file, a message appears informing you that the region will be updated if you proceed.
3. In the applications bar in Crosswork Hierarchical Controller, select **Services > Model Settings**.
4. Select the **Regions** tab.
5. In **Regions**, click  .



6. To import regions in GeoJSON format:
    - Enter the property that includes the region name. Typically, this would be name.
    - Select a file to upload.
7. To import regions in Region POJOs format:
    - Select the Import Region POJOs tab.
    - Select a file to upload.
8. Click **Save uploaded regions**. The JSON file is processed.

9. If there are updates to existing regions, a list of the regions that will be updated appears. To proceed, click **Upload and update regions**.



Regions API

Cisco Sales Engineers will usually set up the regions and overlays in your model. The regions are set up according to the standards published by http://geojson.io/. You can query the model to return the region definition. This returns the region GUID, name, coordinates, and geometry type. Valid geometry types for regions are Point, LineString, Polygon, MultiPoint, MultiLineString, and MultiPolygon.

In Crosswork Hierarchical Controller, devices are attached to sites. Sites have geographical coordinates (latitude, longitude). A site may be in one or more regions.

Overlaps are used to group several regions, for example, the countries in Africa.

There are several APIs that can be used to:

- Get the region definition.
- Get the sites in one or more regions.
- Add regions to an overlay.
- Get the sites in an overlay.

Several samples are listed below:

- To return the RG/1 region definition, run the following GET command:

```
curl -skL -u admin:admin -H 'Content-Type: application/json'
https://$SERVER/api/v2/config/regions/RG/1 | jq
```

- To return the sites in the Estonia and Greece regions:

```
curl -skL -u admin:admin -H 'Content-Type: application/json'
https://$SERVER/api/v2/config/regions/RG/1 | jq
```

- To return the sites in the Estonia and Greece regions:

```
curl -skL -u admin:admin -H 'Content-Type: text/plain'  -d 'region[.name in ("Estonia",
"Greece")] | site' https://$server/api/v2/shql
```

- To add the Estonia and Greece regions to the overlay_europe overlap:

  ```
  curl -X PUT -skL -u admin:admin -H 'Content-Type: application/json' -d '{"guid": "RG/116", "overlay": "overlay_europe"}' https://$SERVER/api/v2/config/regions/RG/116
  ```

  ```
  curl -X PUT -skL -u admin:admin -H 'Content-Type: application/json' -d '{"guid": "RG/154", "overlay": "overlay_europe"}' https://$SERVER/api/v2/config/regions/RG/154
  ```

- To return the sites in the overlay_europe overlay:

  https://$SERVER/api/v2/config/regions/RG/154

  ```
  curl -skL -u admin:admin -H 'Content-Type: text/plain'  -d 'region[.overlay = "overlay_europe"] | site' https://$SERVER/api/v2/shql | jq | grep -c name
  ```

  The regions and overlays can be used in SHQL to query the model. You can transition down the model using link or site.

  ```
  To return all the links in a specific region (using SHQL):
  ```

  ```
  region[.name = "France"] | link
  ```

Sites

Sites are the logical groupings in the network. The Model Settings application enables you to view and filter sites, delete sites, export sites, and import sites. Cisco will usually collaborate with you to set up the sites in your model.

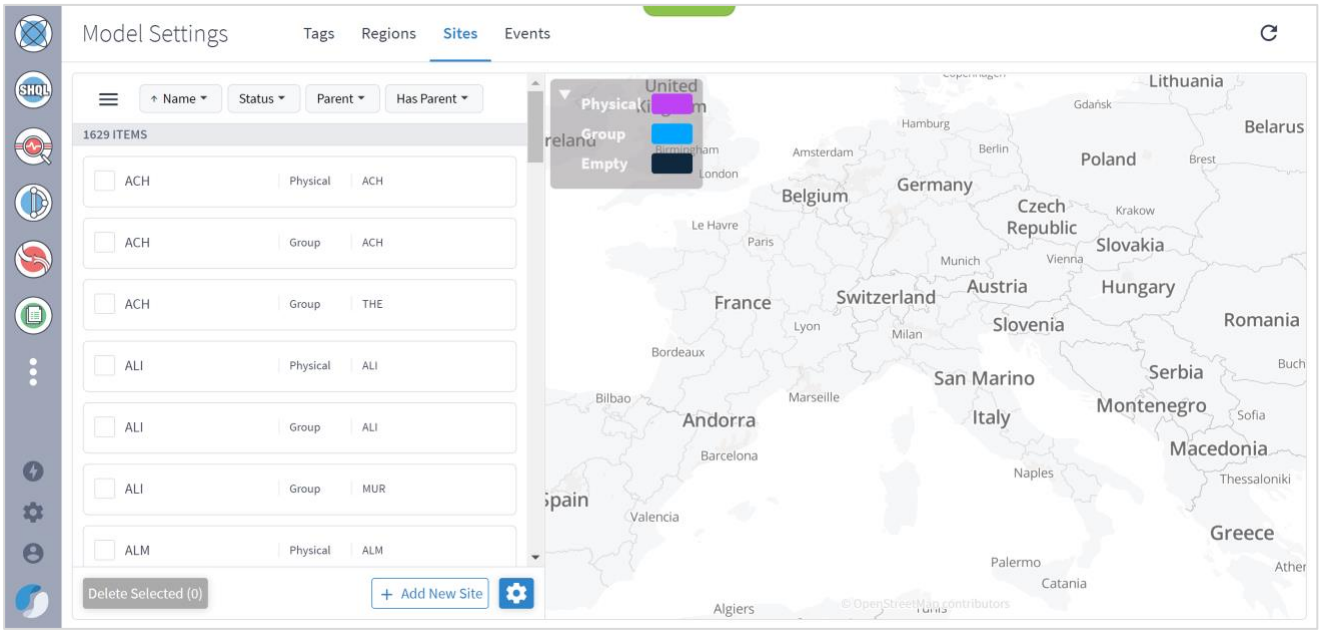
The physical objects in the site can be grouped by parent object, which in turn can be grouped by the next level of parent object, and so on. The only limitation is that all sites must have the same number of levels.

View a Site

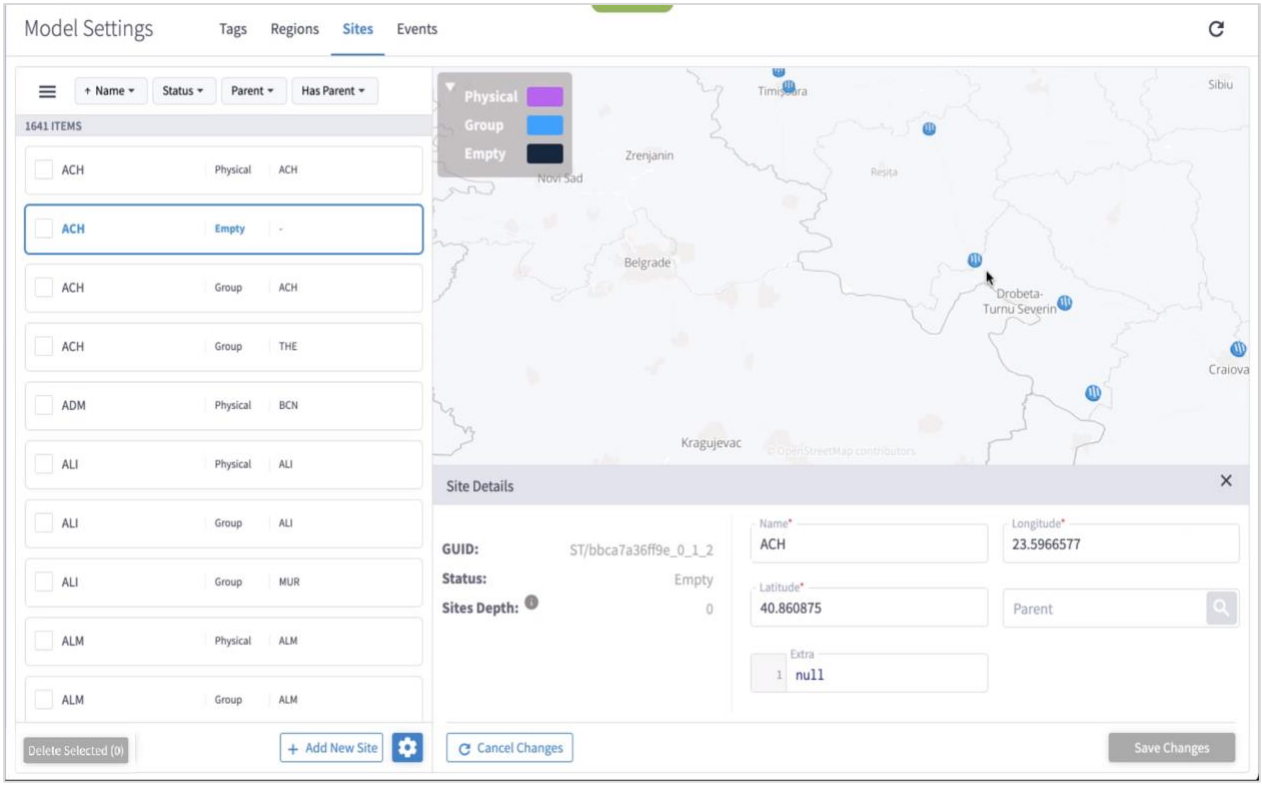
You can view a site in **Model Settings**.

To view a site in Model Settings:

1. In the applications bar in Crosswork Hierarchical Controller, select **Services > Model Settings**.
2. Select the **Sites** tab.



3. To view a site item, in **Sites**, click the required site item. The map moves to the selected site item.

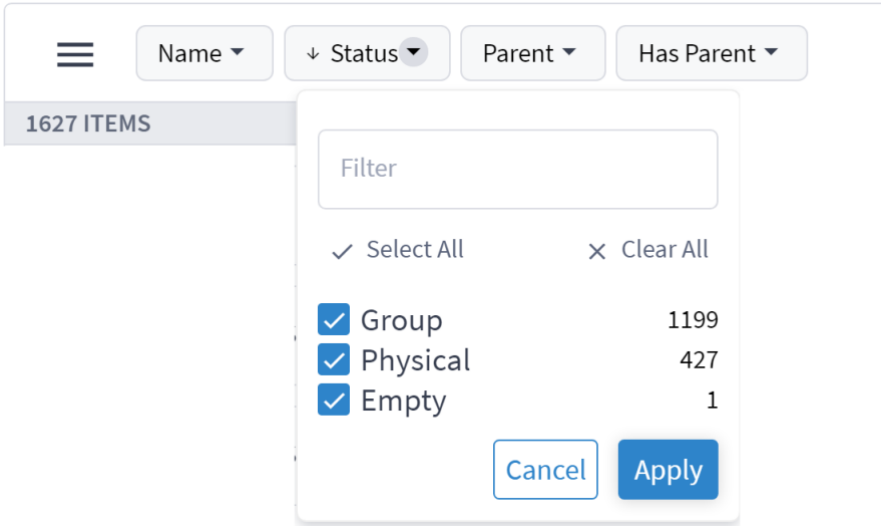


Filter the Sites

You can filter the sites, by name, status, parent or has parent.

To filter a site:

1. In the applications bar in Crosswork Hierarchical Controller, select **Services > Model Settings**.
2. Select the **Sites** tab.
3. To filter the sites, click and select or enter the filter criteria (case insensitive).

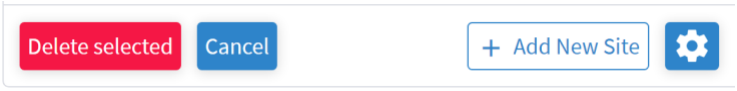


Delete Sites

You can delete sites in Sites Manager.

To delete sites in Sites Manager:

1. In the applications bar in Crosswork Hierarchical Controller, select **Services > Model Settings**.
2. Select the **Sites** tab.
3. In **Sites**, select one or more sites.
4. Click **Delete selected**. A confirmation appears.
5. To delete, click **Delete selected**.

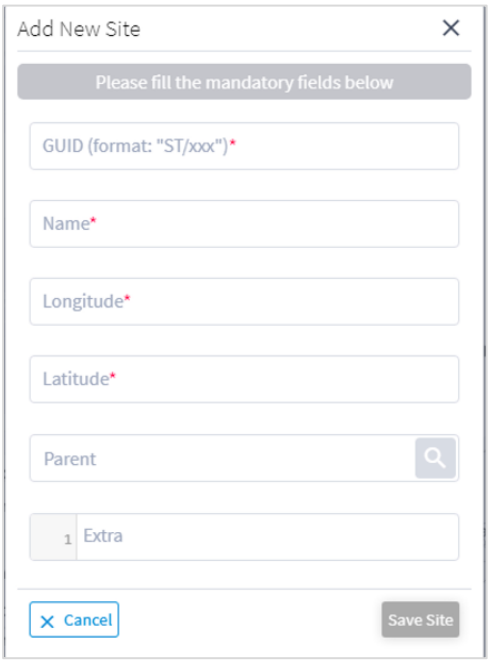


Add Sites

You can add sites in Sites Manager.

To add sites in Sites Manager:

1. In the applications bar in Crosswork Hierarchical Controller, select **Services > Model Settings**.
2. Select the **Sites** tab.
3. Click **Add New Site**.



4. Enter the site details. For example, **ST/London**.
5. Click **Save Site**.

Export and Import Sites

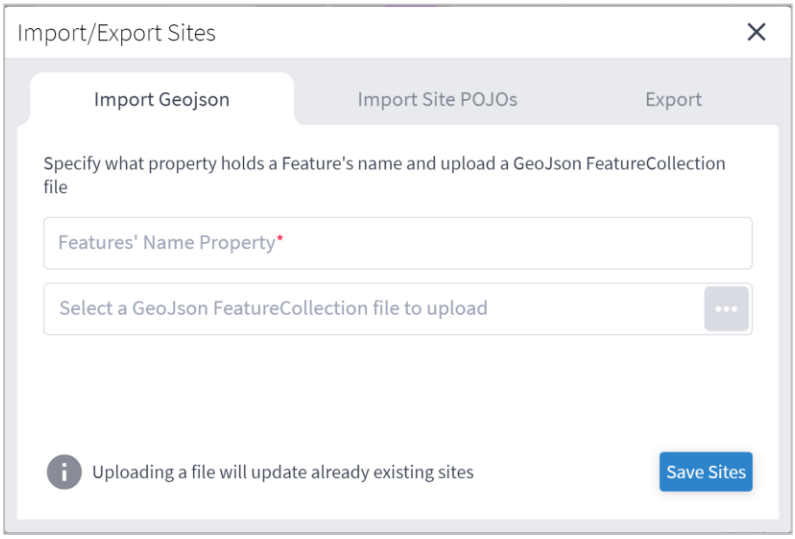
Cisco will usually collaborate with you to set up the sites in your model. The sites are set up according to the standards published by http://geojson.io/ and can be exported or imported in GeoJSON or Site POJOs.

You can import (and export) sites in the following formats:

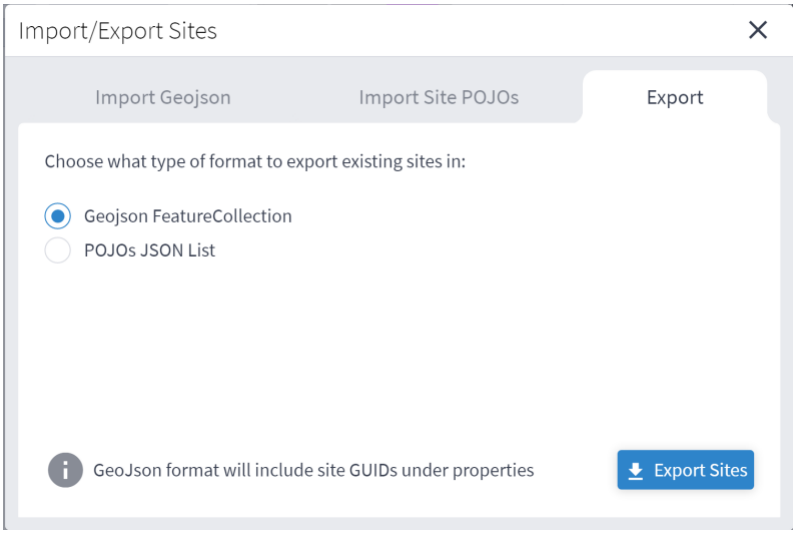
- GeoJSON
- Site POJOs

To export sites:

1. In the applications bar in Crosswork Hierarchical Controller, select **Services > Model Settings**.
2. Select the **Sites** tab.
3. In **Sites**, click .



4. To export In **Sites**, select the **Export** tab.



5. Select the required format, and then click **Export sites** . The **netfusion-sites-geojson.json** file is downloaded.
6. (Optional) Use a JSON formatter to review the content.

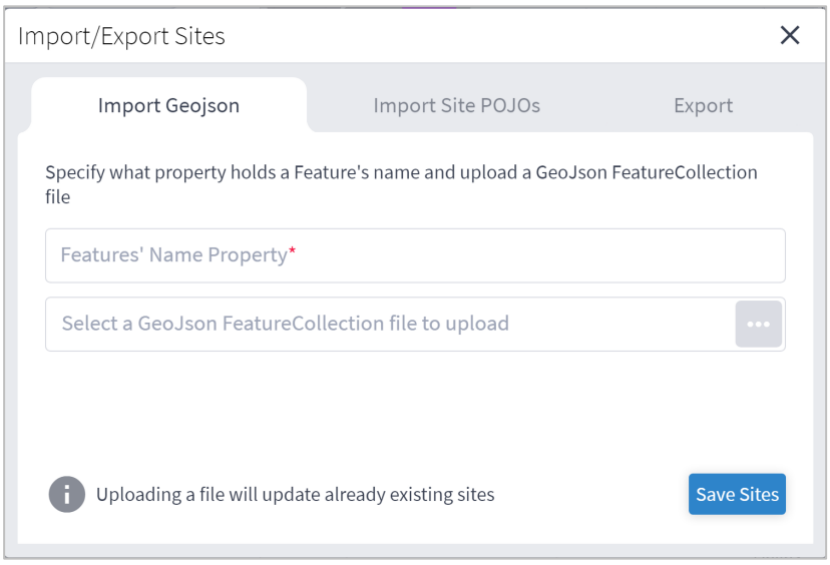
```
{
  "site": [
    {
      "guid": "ST/001ca9f0dc37",
      "latitude": 51.5105384,
      "longitude": -0.5950406,
      "name": "SLO",
      "parent": {
        "guid": "ST/001ca9f0dc37_0"
      },
      "extra": null
    },
    {
      "guid": "ST/001ca9f0dc37_0",
      "latitude": 51.5105384,
      "longitude": -0.5950406,
      "name": "SLO",
      "parent": {
        "guid": "ST/2971737bd3ba_0_1"
      },
      "extra": null
    },
    {
      "guid": "ST/002d237f16fb8c65",
      "latitude": 37.9020842,
      "longitude": -6.5648524,
      "name": "ILA-SD1EVO01-SD1SEV01-1",
      "parent": {
        "guid": "ST/002d237f16fb8c65_0"
      },
      "extra": null
    },
    {
      "guid": "ST/002d237f16fb8c65_0",
      "latitude": 37.9020842,
      "longitude": -6.5648524,
      "name": "ILA-SD1EVO01-SD1SEV01-1",
```

To import sites:

1. (Option 1) Prepare the import file in **GeoJSON** format:
   - A quick way to create the file in the correct format is to export the current sites in the required format and then edit the file.
   - The GeoJSON import file must be a **FeatureCollection** GeoJSON file and not a single **Feature** GeoJSON file.
   - The GeoJSON import file MUST have a site name property that will be specified when you import the file.
   - The GeoJSON import file may include a GUID for each site. If a GUID is not provided, Sites Manager, generates a GUID for the GeoJSON feature. If a GUID is provided, Sites Manager uses it, and if a site with that GUID already exists it is updated.
   - Each site name (and GUID if included) must only appear once.
   - Site names are case insensitive.

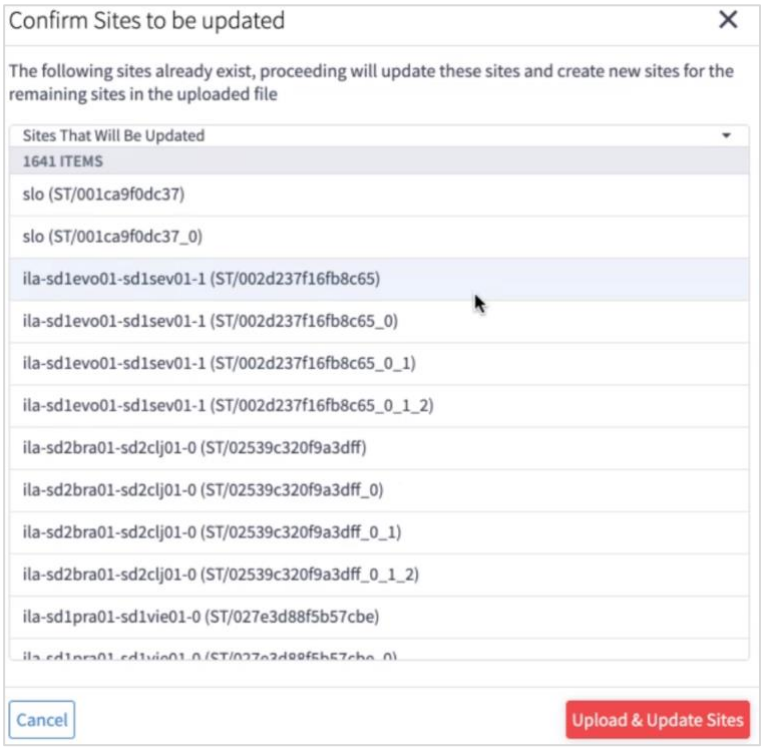
- If a site already exists either by GUID or with an identical name, when you import the file, a message appears informing you that the site will be updated if you proceed.

2. (Option 2) Prepare the import file in Site POJOs format:
   - A quick way to create the file in the correct format is to export the current sites in the required format and then edit the file.
   - The SitePOJO import file has a fixed format and the site name property is **name**. This property does not have to be specified when you import the file.
   - The SitePOJO import file must include the site GUID as a property.
   - Each site name and GUID must only appear once.
   - Site names are case insensitive.
   - If a site already exists (by name or GUID), when you import the file, a message appears informing you that the site will be updated if you proceed.
3. In the applications bar in Crosswork Hierarchical Controller, select **Services > Model Settings**.
4. Select the **Sites** tab.
5. In **Sites**, click .



6. To import sites in GeoJSON format:
   - Enter the property that includes the site name. Typically, this would be name.
   - Select a file to upload.
7. To import sites in Site POJOs format:
   - Select the **Import Site POJOs** tab.
   - Select a file to upload.
8. Click **Save uploaded sites**. The JSON file is processed.

9. If there are updates to existing sites, a list of the sites that will be updated appears. To proceed, click **Upload and Update Sites**.

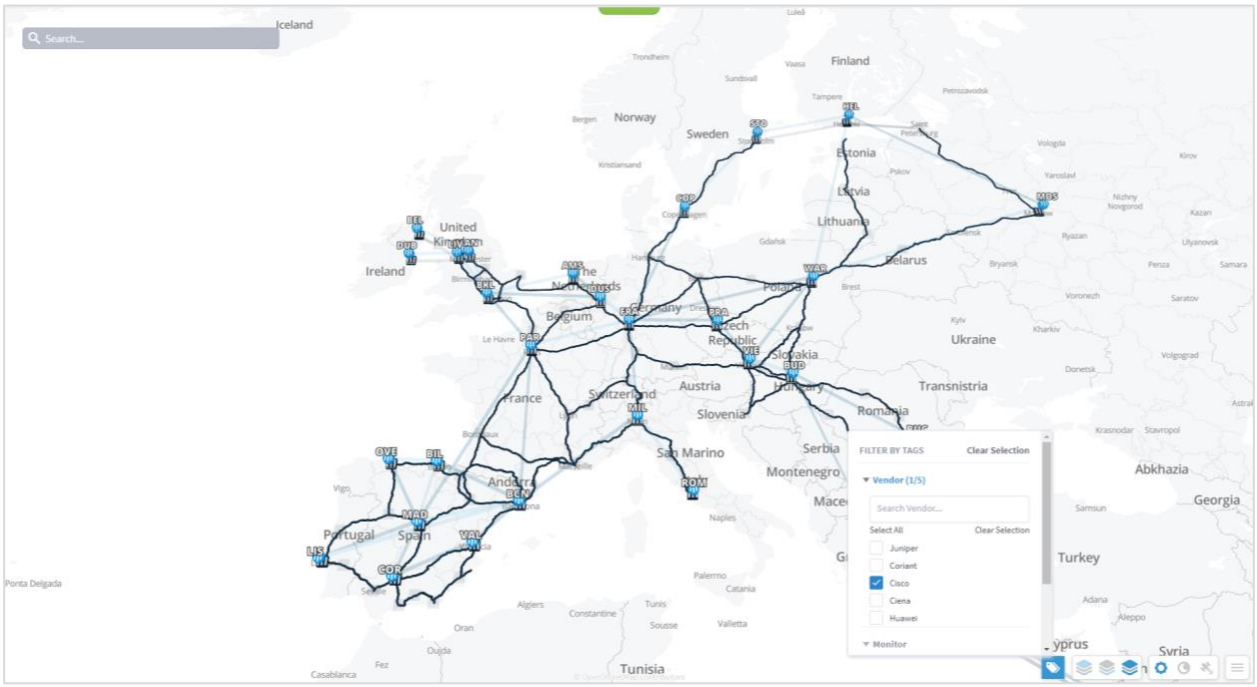


Tags

Resources can be tagged with a text label (using key:value pair). You can view, add, or delete tags in the Model Settings application (or using the Tags API).

Tags can be used as follows:

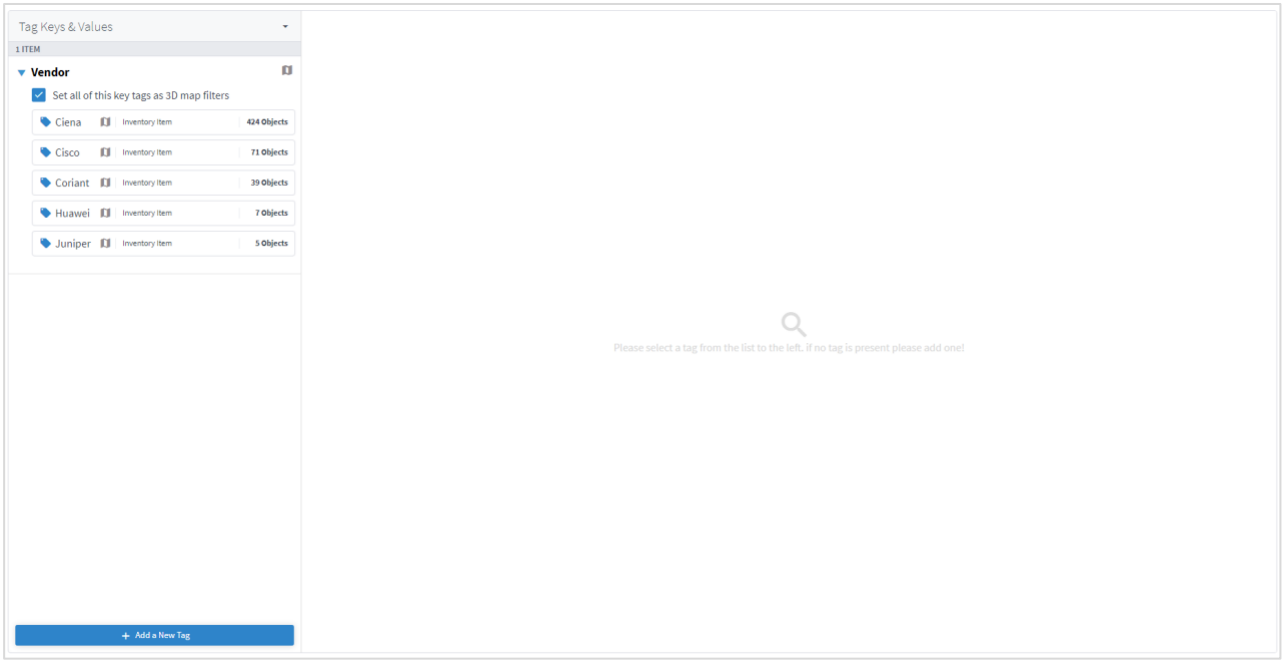
- In Explorer, for example, you can filter the 3D map by links tags – this applies to the links that are visible in the map (logical, OMS), and you can select which tags to use as a map filter.
- In the Network Inventory application, you can show tags as columns.
- In the Path Optimization application, you can run a test on tagged links, and exclude tagged links from the path.
- In the Network Vulnerability application, you can run a test on tagged routers.
- In the Root Cause Analysis application, you can filter results by tag.



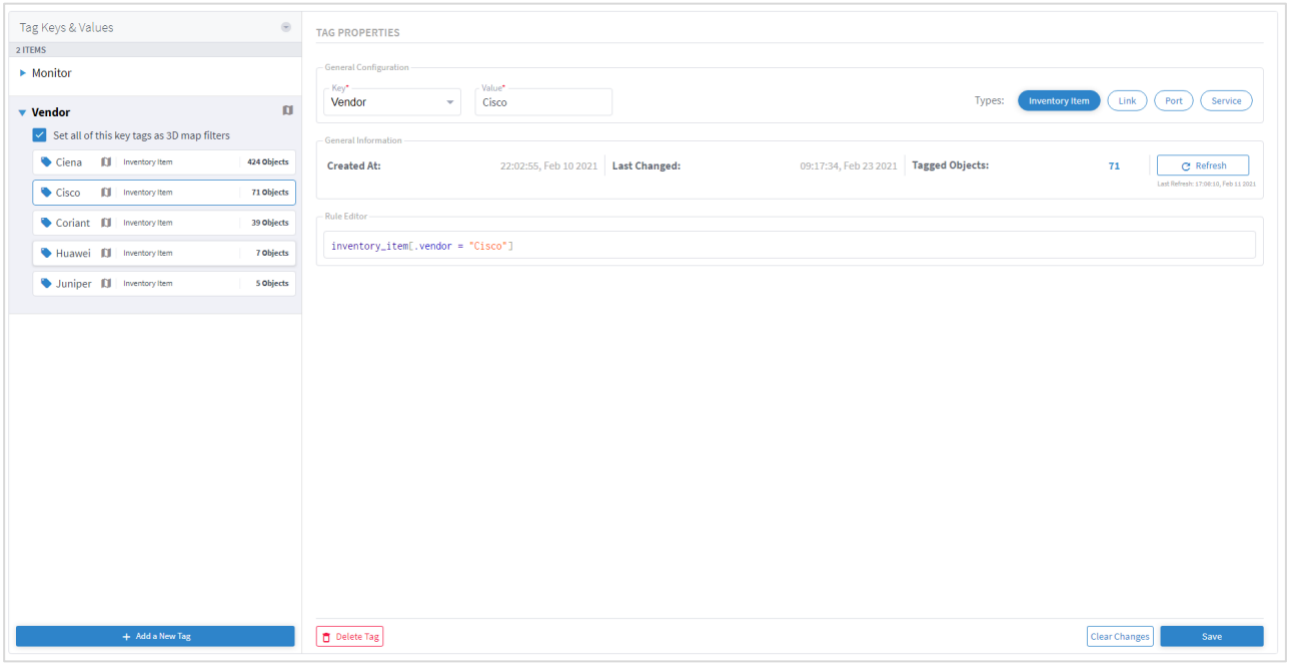
View the Tags

To view the tags in Model Settings:

1. In the applications bar in Crosswork Hierarchical Controller, select **Services > Model Settings**.
2. Select the **Tags** tab.



3. To view the tags, expand the tag key and select the value, for example, expand **Vendor**.

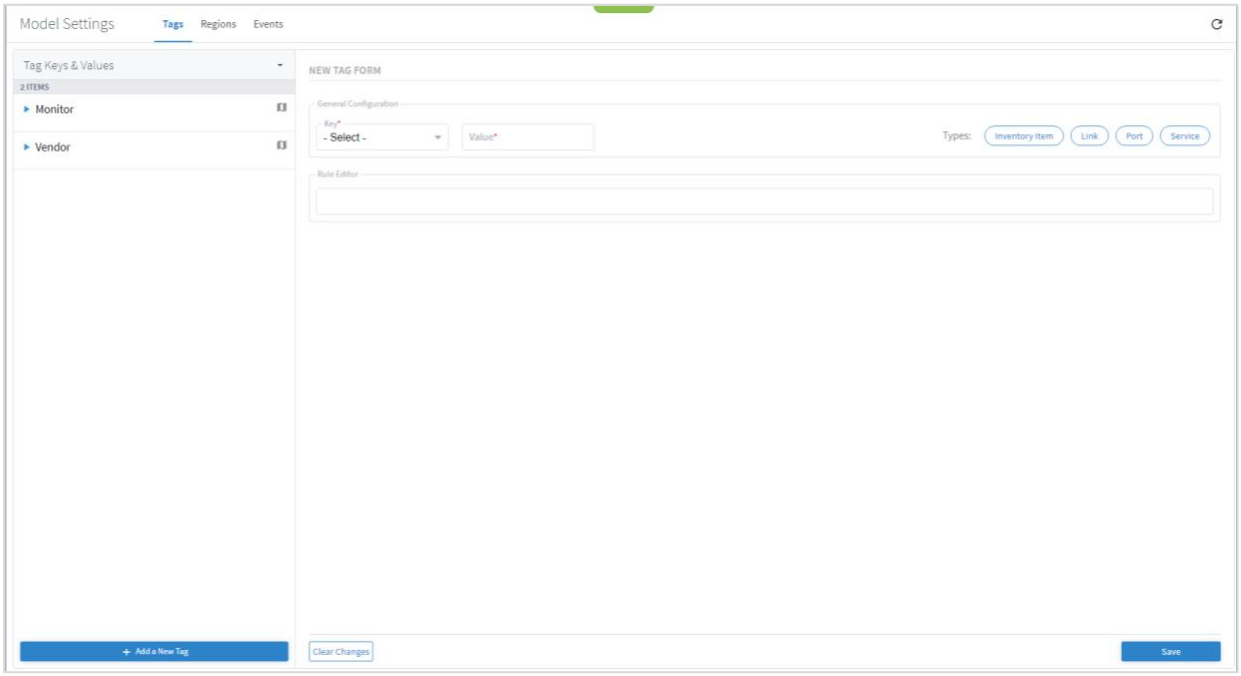


Add Tags

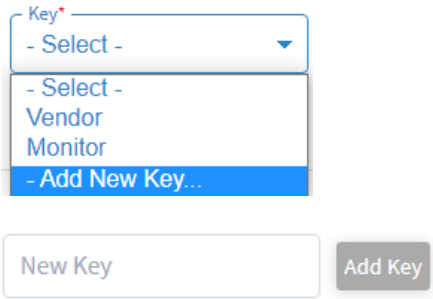
You can add a new value to an existing tag, or add a new tag.

To add tags in Model Settings:

1. In the applications bar in Crosswork Hierarchical Controller, **select Services > Model Settings**.
2. Select the **Tags** tab.
3. Click **Add a New Tag**.

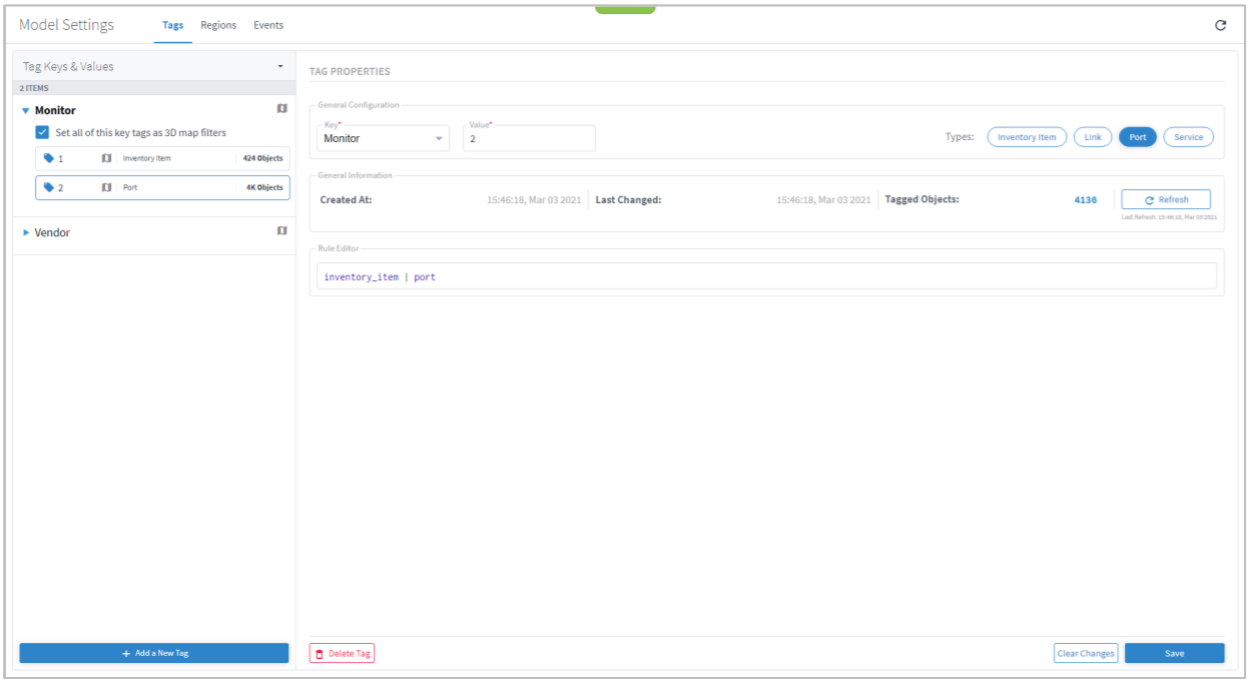


4. To add a new key, from the **Key** dropdown, select **Add New Key**.



5. Enter a key name and click **Add Key**.
6. To add a new value to an existing key, from the **Key** dropdown select an existing key, and then enter a new **Value**.

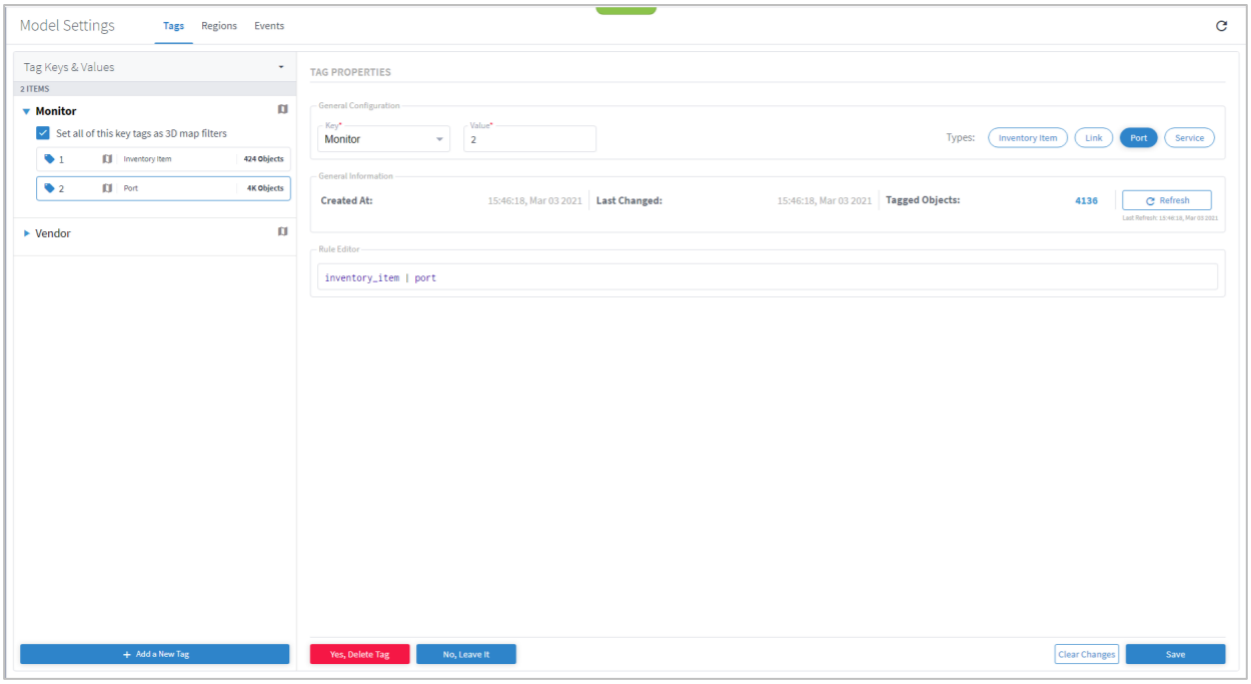
7. In the **Rule Editor**, select the required resources to apply the key and value to, for example, **inventory_item** | port and then click **Save**. The key entry is added, and you can see how many objects are tagged.



Delete Tags

To delete tags in Model Settings:

1. In the applications bar in Crosswork Hierarchical Controller, select **Services > Model Settings**.
2. Select the **Tags** tab.
3. Expand the required tag key and select a tag value.
4. Click **Delete Tag**.



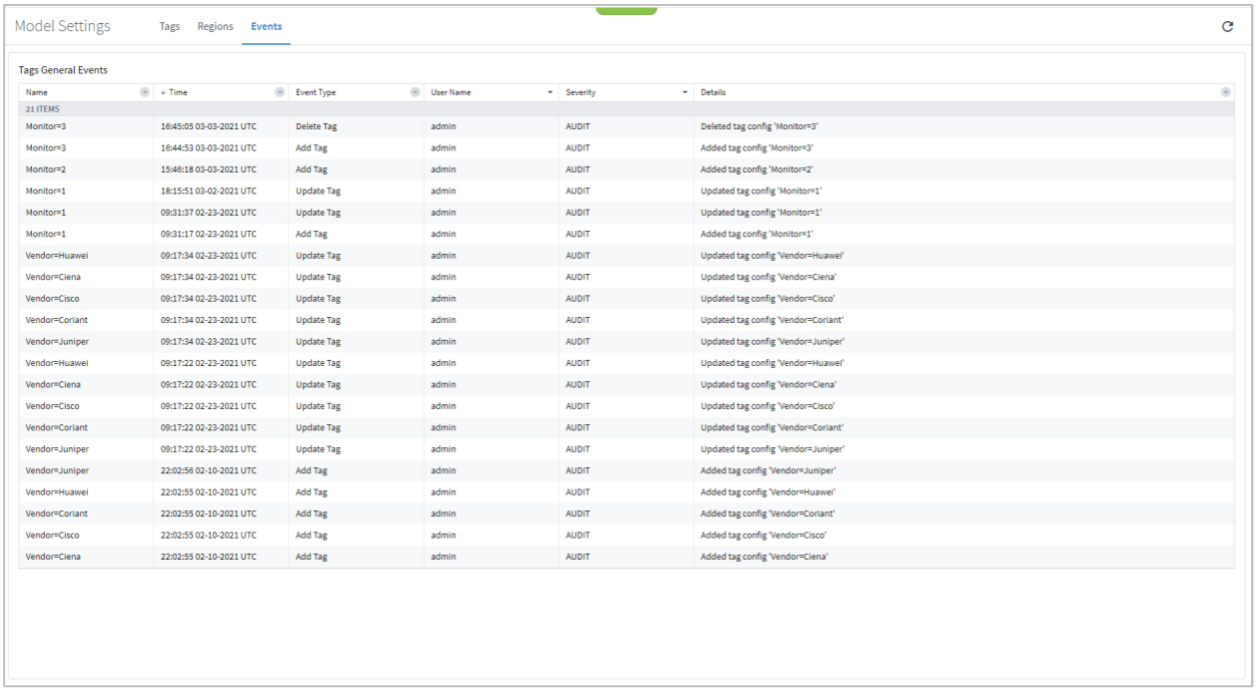
5. Click **Yes, Delete Tag**.

View Tag Events

You can view a list add, update, and delete tag events.

To view tag events in Model Settings:

1. In the applications bar in Crosswork Hierarchical Controller, select **Services > Model Settings**.
2. Select the **Events** tab.



Tags API

Tags can also be added or changed by API or SHQL.

Get Devices by Tags

You can get devices by tags using the SHQL app.

- To return all devices that are tagged with the Vendor tag set to Ciena (using SHQL):

```
inventory[.tags.Vendor has ("Ciena")]
```

Add Tag to Device

You can create a tag and assign the tag with a value to a device (or several devices) using the tags API. This API uses an SHQL rule as a parameter. All devices returned by the SHQL rule are tagged with the specified value. For example, this creates a Vendor tag and assigns the value Ciena to all the inventory items with vendor equal to Ciena.

```
POST "https://$SERVER/api/v2/config/tags" -H 'Content-Type: application/json' -d "{
    \"category\": \"Vendor\",
    \"value\": \"Ciena\",
    \"rules\": [
         \"inventory_item[.vendor = Error! Hyperlink reference not valid."
 }"
```

Parameter	Description
category	The tag category, for example, **Vendor**.
value	The value to tag the device with, for example, **Ciena**.
rules	The SHQL rule to apply. The rule MUST return items. Use the following in the rules: regions, tags, site, inventory.

For example, you can add tags to devices by using a query that returns all devices in a specific region:

```
POST  "https://$SERVER/api/v2/config/tags" -H 'Content-Type: application/json' -d "{
     \"category\": \"Region\",
     \"value\": \"RG_2\",
     \"rules\": [
          \"region[.guid = \\\"RG/2\\\"] | site | inventory\"
     ]
  }"
```

Delete Tag

You can delete a tag.

```
DELETE "https://$SERVER/api/v2/config/tags/Vendor=Ciena"
```

Managed Devices

The following statuses are available per device (and as a total for all the devices) in the **Managed Devices** table in Device Manager.

	Information Types		
Possible values	**Inventory**	**Topology**	**Statistics**
OK	When the adapter collecting the specific info type successfully reached the device NMS system or device itself and discovered the device data.		
ERROR	When the adapter collecting the info type reached the device but could not collect the required information, for example, wrong credentials, command type error, or no data.		
UNREACHABLE	When the adapter collecting the info type failed to reach the device, typically as a result of a problem with connectivity.		
WARNING	N/A	N/A	When the adapter that collects statistics failed to get the data of some device ports.
UNKNOWN	When no status was reported by the adapter. This occurs when there is an internal communication error. Refer this to support.		

Crosswork Hierarchical Controller sends SYSLOG events when the device reachability state changes.

You can add devices and assign them to adapters.

Link Management

The Link Manager application enables you to manually add and validate inter-links (or cross-links) from IP to optical networks or from Transponder/Muxponder to OLS. The links added by the user in the application are merged into the Crosswork Hierarchical Controller network model.

You can add Ethernet and NMC cross links manually:

- Ethernet links - IP to optical
- NMC link - xPonder to OLS

The links are validated:

- When a link is added, or the link status changes
- Periodically (per the configured cycle time)
- Manually by the user

Note: Link validation is for Ethernet links only and is achieved by analyzing PM counters received on the link ports.

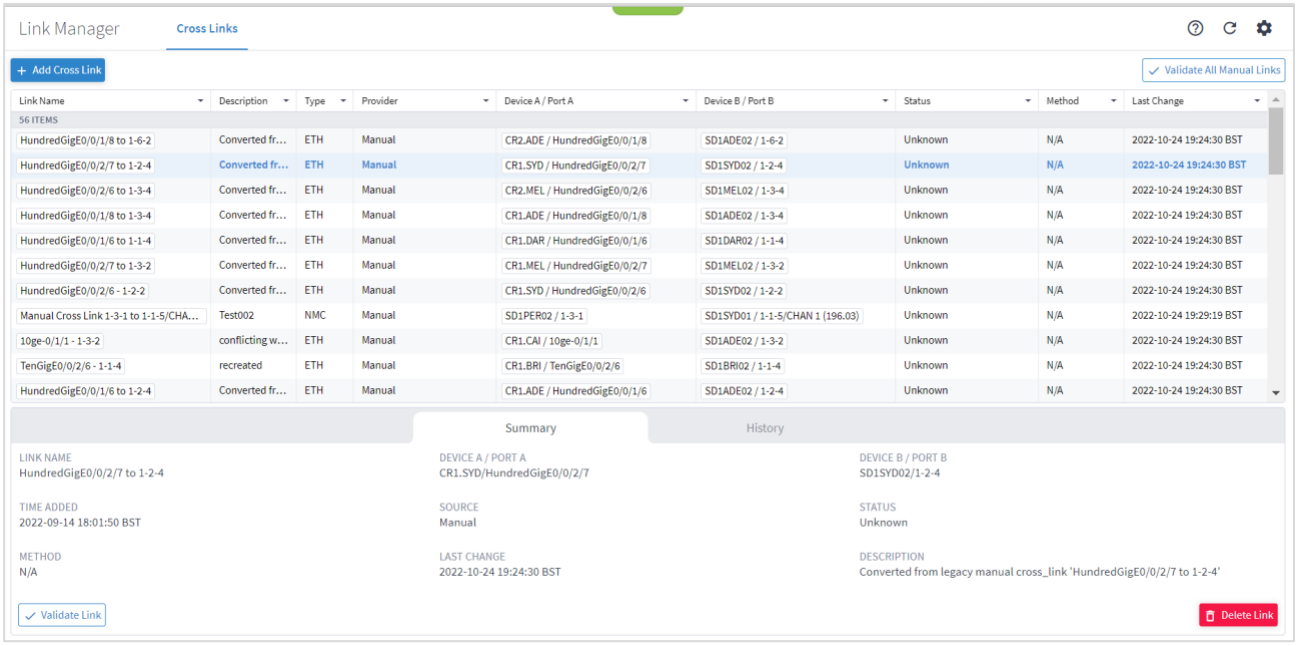
View Cross Link Info

You can select a cross link and view the summary information. The **Provider** column indicates whether the cross link was manually added or detected by the network, and the **Status** indicates whether the cross link is **Unknown** (added manually or by an adapter and not yet validated), **Validated**, or **Unlikely** (validation failed, mismatch with another validated cross-link).

To view the cross link info:

1. In the applications bar in Crosswork Hierarchical Controller, select **Link Manager**.

2. Click on a cross link.

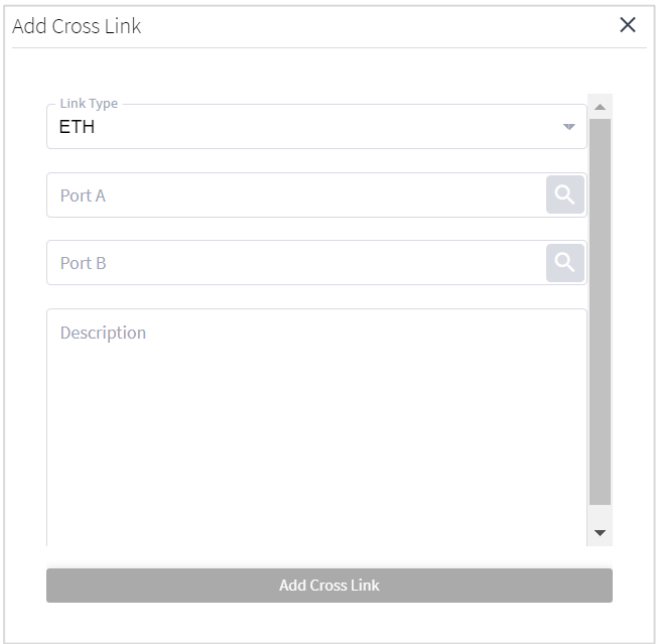


Add a Cross Link

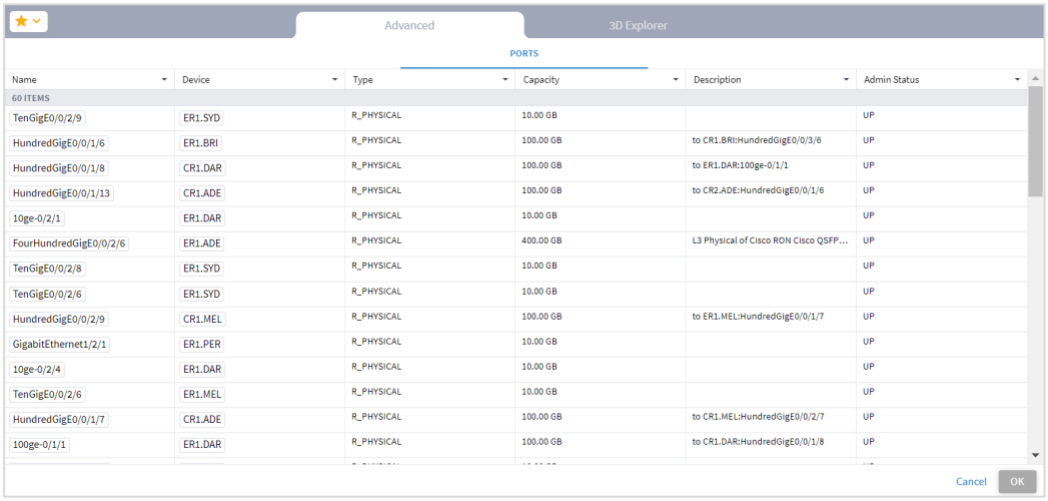
You can add an Ethernet or NMC cross link.

To add a cross link:

1. In the applications bar in Crosswork Hierarchical Controller, select **Link Manager**.
2. Click **Add Cross Link**.



3. To add link, in the **Link Type**, select **ETH** or **NMC**.
4. For **Port A** and **Port B**, click . In the **Ports** tab, select a port, or click on the **3D Explorer** tab to select a port. Click **OK**. For NMC cross links



Note: For more information on 3D Explorer, see the *Cisco Crosswork Hierarchical Controller Network Visualization Guide*.

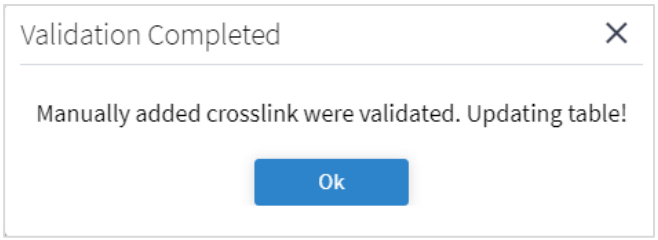
5. Add a **Description**.
6. Click **Add Cross Link**.

Validate All Manual Cross Links

You can validate all manual cross links. For an Ethernet link, if there is a conflict between a manually added cross link and a cross link detected from the network, the manually added link is removed from Cisco Crosswork Hierarchical Controller network model. Such links remain in a separate table, and you can view them in the Link Manager application. This also removes all cross links that are marked as deleted.

To validate manual cross links:

1. In the applications bar in Crosswork Hierarchical Controller, select **Link Manager**.
2. Click **Validate all Manual Links**. The **Status** is updated.



3. Click **OK**.

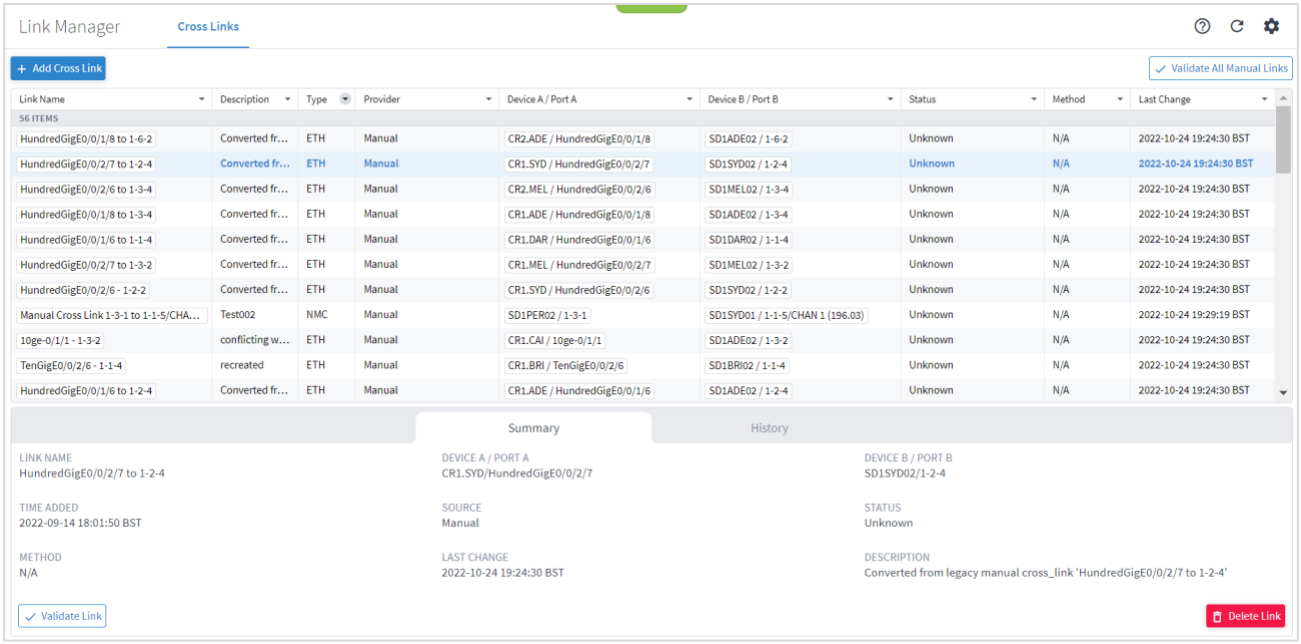
Validate a Manual Cross Link

You can validate a manual cross link. In version 6.0, you can only validate Ethernet links.

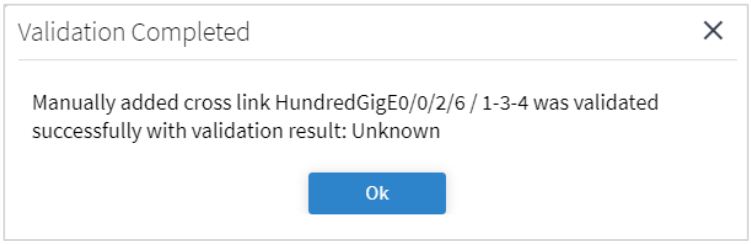
To validate a manual cross link:

1. In the applications bar in Crosswork Hierarchical Controller, select **Link Manager**.

2. Select the required manual link.



3. In the lower pane, click **Validate Link**.



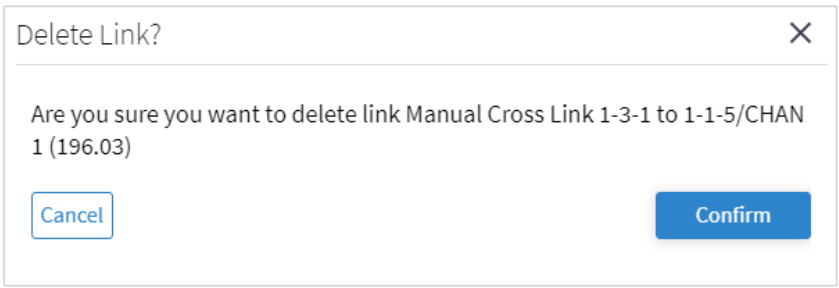
4. Click **Ok**.

Delete a Cross Link

You can delete a manual cross link. The cross link is marked as deleted and is removed when the next validation runs.

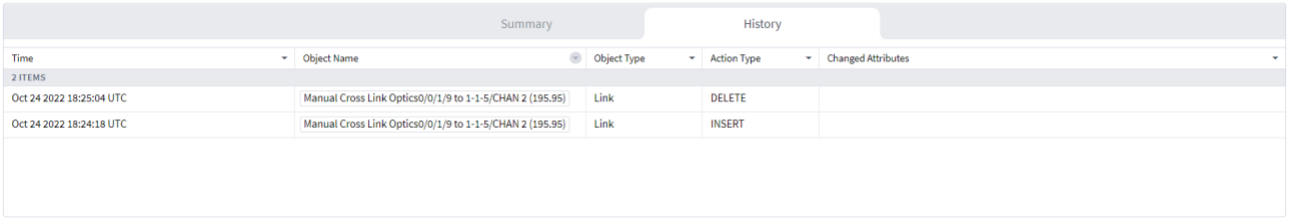
To delete a manual cross link:

1. In the applications bar in Crosswork Hierarchical Controller, select **Link Manager**.
2. Select the required manual link.
3. In the lower pane, click **Delete Link**.



4. Click **Confirm**.

5. Click **Ok**.
6. Select the deleted cross link and click on the **History** tab to view the **DELETE** action.



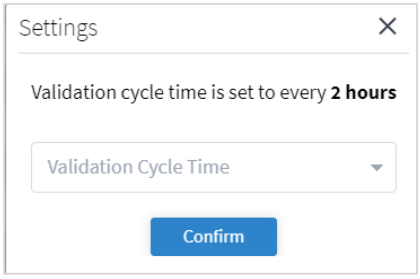
The link removed when the next validation runs.

Set Validation Cycle Time

You can set the validation cycle time.

To set the validation cycle time:

1. In the applications bar in Crosswork Hierarchical Controller, select **Link Manager**.
2. Click ⚙.



3. Select the **Validation Cycle Time**.
4. Click **Confirm**.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA 10/22