Onboard and Manage Devices

This section contains the following topics:

Add Devices to the Inventory

There are different ways to add devices to Crosswork. Each has its own set of prerequisites, which you must fulfill if the device addition is to succeed. Ensure that your devices are configured properly for communication and telemetry. See guidelines and example configurations in Telemetry Prerequisites for New Devices, on page 2 and Sample Configuration for Cisco NSO Devices, on page 7.

In order of preference for most users, the methods and their prerequisites are:

1. **Importing devices using the Crosswork APIs:** : This is the fastest and most efficient of all the methods, but requires programming skills and API knowledge. For more, see the Inventory Management APIs On Cisco Devnet.

2. **Importing devices from a Devices CSV file**: This method can be time-consuming. To succeed with this method, you must first:

    - Create the provider(s) that will be associated with the devices. See About Adding Providers.

    - Create corresponding credential profiles for all of the devices and providers listed in the CSV file. See Create Credential Profiles.

    - Create tags for use in grouping the new devices. See Create Tags.

    - Download the CSV template file from Crosswork and populate it with all the devices you will need.

3. **Adding them via the UI**: This method is the least error-prone of the three methods, as all data is validated during entry. It is also the most time-consuming, being suitable only for adding a few devices at a time.

Note that the providers, credential profiles and tags you want to apply to them must exist beforehand. For more information, see Add Devices through the UI, on page 8.

4. **Auto-onboarding from a Cisco SR-PCE provider**: This method is highly automated and relatively simple. Note that the device and provider credential profiles and tags you want to apply to these devices must exist beforehand. After onboarding devices from this source, you will need to edit each device to add device information that is not automatically discovered. For more information, see the provider properties in Add Cisco SR-PCE Providers.

5. **Auto-onboarding using Zero Touch Provisioning**: This method is automated, but requires that you create device entries first and modify your installation's DHCP server. Note that the device and provider credential profiles and tags you want to apply to these devices must exist beforehand. After provisioning and onboarding devices using this method, you will need to edit each device to add information that is not automatically supplied. For more information, see Zero Touch Provisioning.

Note

Cisco Crosswork only supports single-stack deployment modes. The devices can be onboarded with either an IPv4 address or an IPv6 address, not both.

If a device onboarded in Cisco Crosswork is on the same subnet as a Cisco Crosswork Data Gateway interface, then it must be on the Cisco Crosswork Data Gateway's southbound network. This is because Cisco Crosswork Data Gateway implements RPF checks and the source address of devices cannot be on the management or northbound networks if multitple NICs (2 or 3 NIC) are deployed.

Telemetry Prerequisites for New Devices

Before onboarding new devices, you must ensure that the devices are configured to collect and transmit telemetry data successfully with Cisco Crosswork. The following sections provide sample configurations for several telemetry options, including SNMP, NETCONF, SSH and Telnet. Use them as a guide to configuring the devices you plan to manage.

Note

- SNMPv2 and SNMPv3 (Auth/Priv) traps are supported.
- For the device to work seamlessly in Crosswork, the SNMP EngineID generated/configured in the device should be unique in the network.
- For the credentials to work, SNMP users should be re-created if the SNMP EngineID is re-configured in the device.

Configure Devices to Forward Events to Crosswork

To ensure that Crosswork can query devices and receive events and notifications from them, you must configure devices to forward events to the Crosswork server. For most devices, this means you must configure the devices to forward SNMP traps and syslogs, and the Data Gateway IP acts as the receiver IP.

For other devices (such as some optical devices), it means you must configure the devices to forward TL1 messages.

If you have a high availability deployment, you must configure devices to forward events to both the primary and secondary servers (unless you are using a virtual IP address).

In most cases, you should configure this using the **snmp-server host** command.

Pre-Onboarding Device Configuration

The following commands provide a sample pre-onboarding device configuration that sets the correct SNMPv2 and NETCONF configuration, and SSH and Telnet rate limits. The NETCONF setting is only needed if the device is MDT-capable.

Warning During Service Health monitoring, the IOS XR version 7.8.1 or later device responds with duplicate values. This disrupts the data collection process and results in the error message 'unable to acquire feed' as it attempts to retrieve the interface health status. You can prevent this issue by defining the packet size for the SNMP server through `snmp-server packetsize 4096`.

```
logging console debugging
logging monitor debugging
telnet vrf default ipv4 server max-servers 100
telnet vrf default ipv6 server max-servers 100
crypto key generate rsa
 exec-timeout 0 0
 width 107
 length 37
 absolute-timeout 0
!
snmp-server community public RO
snmp-server community robot-demo2 RO
snmp-server ifindex persist
snmp-server packetsize 4096
ntp
 server <NTPServerIPAddress>
!
ssh server v2
ssh server vrf default
ssh server netconf vrf default
ssh server logging
ssh server rate-limit 100
ssh server session-limit 100
!
netconf agent tty
!
netconf-yang agent
 ssh
!
```

SNMPv3 Pre-Onboarding Device Configuration

If you want to enable SNMPv3 data collection, repeat the SNMPv2 configuration commands in the previous section, and add the following commands:

```
snmp-server group grpauthpriv v3 priv notify v1default
snmp-server user <user-ID> grpauthpriv v3 auth md5 <password> priv aes 128 <password>
```

Pre-Onboarding SNMPv2 and SNMPv3 Trap Configuration

If you want the device to send SNMP traps to Cisco Crosswork, use the following commands to perform a pre-onboarding device configuration and test for the trap version you want.

For SNMP v2 traps:

```
snmp-server trap link ietf
snmp-server host <CrossworkDataGatewaySouthboundIPAddress> traps version 2c cisco123 udp-port
 1062
snmp-server community cisco123
snmp-server traps snmp linkup
snmp-server traps snmp linkdown
```

For SNMP v3 traps:

```
snmp-server trap link ietf
snmp-server host <CrossworkDataGatewaySouthboundIPAddress> traps version 3 cisco123 udp-port
 1062
snmp-server community cisco123
snmp-server traps snmp linkup
snmp-server traps snmp linkdown
```

Please note that, for traps to be received, the node_ip field for the device as listed in the Cisco Crosswork inventory must match the IP address of the device interface from which the traps are sent. If they do not, Cisco Crosswork will reject the traps. Also, the device needs to be in ADMIN_UP state for traps to be received.

Required Settings—Cisco IOS and IOS-XE Device Operating System

```
snmp-server host cdg_virtualIP
snmp-server community public-cmty RO
snmp-server community private-cmty RW
snmp-server ifindex persist

logging cdg_virtualIP
logging on
logging buffered 64000 informational

logging source-interface interface_name
logging trap informational
logging event link-status default
```

Note The *cdg_virtualIP* denotes the virtual IP address used in the Crosswork Data Gateway pool creation.

Disable domain lookups to avoid delay in Telnet/SSH command response:

```
no ip domain-lookup
```

Enable SSH

```
crypto key generate rsa
ip ssh rsa keypair-name keypair-name
crypto key generate rsa usage-keys label key-label modulus modulus-size
ip ssh version [1 | 2]
```

Setup VTY options:

```
line vty <number of vty>
exec-timeout
session-timeout
transport input ssh (requird only if ssh is used)
transport output ssh (required only if ssh isused)
```

Enable CFM modeling:

```
snmp-server view all 1.3.111.2.802.1.1.8 included
```

For SNMPv2 only, configure the community string:

```
snmp-server community ReadonlyCommunityName RO
```

For SNMPv3 only, configure the following settings:

```
snmp-server user User Group v3 auth sha Password priv des Password
snmp-server view Group 1.3.6 included
snmp-server view Group 1.0.8802.1.1.2 included
snmp-server group Group v3 priv notify Group read Group

snmp-server group Group v3 priv read v1default write v1default notify v1default
snmp-server group Group v3 priv
snmp-server group Group v3 priv notify crosswork read crosswork
```

Note

- For the device to work seamlessly in Crosswork, the SNMP EngineID generated/configured in the device should be unique in the network.
- For the credentials to work, SNMP users should be re-created if the SNMP EngineID is re-configured in the device.

Configure the cache settings at a global level to improve the SNMP interface response time using the configuration:

```
snmp-server cache
```

Syslogs are used by Crosswork for alarm and event management. NTP settings ensure that Crosswork receives the correct timestamps for events. To configure syslogs on the device, add the following settings:

```
clock timezone TimeZone
service timestamps log datetime show-timezone msec year
ntp server NTP_Server
update-calendar
logging facility local7
logging cdg_virtualIP vrf default severity info [port default]
```

Required Settings—Cisco IOS XR Device Operating System

```
snmp-server community community_name SystemOwner
snmp-server community community_name RO
snmp-server entityindex persist
snmp-server ifindex persist

logging cdg_virtualIP
logging on
logging buffered <307200-125000000>

logging source-interface interface_name

logging trap informational
logging events level informational
logging events link-status
logging events link-status software-interfaces

no cli whitespace completion
domain ipv4 host server_name cdg_virtualIP
```

Set up VTY options:

```
line default
exec-timeout 10 0
session-limit 10
session-timeout 100
transport input ssh
transport output ssh
vty-pool default 0 99 line-template default
```

Telnet and SSH Settings:

```
telnet ipv4 server max-servers no-limit
telnet vrf default ipv4 server max-servers 100
ssh server v2
ssh server rate-limit 60
cinetd rate-limit 60
```

Configure the Netconf and XML agents:

```
xml agent tty
netconf agent tty
```

Monitor device with Virtual IP address :

```
ipv4 virtual address use-as-src-addr
ipv4 virtual address Virtual_IP_Address/Subnet_Mask
```

Enable CFM modeling:

```
snmp-server view all 1.3.111.2.802.1.1.8 included
```

For SNMPv2 only, configure the community string:

```
snmp-server community ReadonlyCommunityName RO SystemOwner
```

For SNMPv3 only, configure the following settings:

```
snmp-server user User Group v3 auth sha encrypted Password priv des56 encrypted
Password SystemOwner
snmp-server view Group 1.3.6 included
snmp-server view Group 1.0.8802.1.1.2 included
snmp-server group Group v3 priv notify Group read Group
snmp-server group Group v3 priv read v1default write v1default notify v1default
```

Configure the following to improve the SNMP interface stats response time:

```
snmp-server ifmib stats cache
```

Configure SNMP traps for virtual interfaces to ensure that link-down scenarios are captured:

```
snmp-server interface subset 2 regular-expression Forty*
notification linkupdown
!
snmp-server interface subset 3 regular-expression Ten*
notification linkupdown
!
snmp-server interface subset 1 regular-expression Hun*
notification linkupdown
!
snmp-server interface subset 1 regular-expression TwoHun*
notification linkupdown
!
snmp-server interface subset 1 regular-expression FourHun*
notification linkupdown
```

Enable SNMP entity field replaceable unit (FRU) control traps:

```
snmp-server traps fru-ctrl
```

Syslogs are used by Crosswork for alarm and event management. NTP settings ensure that Crosswork receives the correct timestamps for events. To configure syslogs on the device, add the following settings:

```
clock timezone TimeZone
service timestamps log datetime show-timezone msec year
ntp server NTP_Server
logging facility local7
logging cdg_virtualIP vrf name
```

Enable performance management on all optical data unit (ODU) controllers:

```
controller oduX R/S/I/P
per-mon enable
```

Enable performance management for Tandem Connection Monitoring (TCM):

```
tcm id {1-6}
perf-mon enable
```

To open Cisco Transport Controller (CTC) from Crosswork, enable the HTTP/HTTPS server:

```
http server ssl
```

Sample Configuration for Cisco NSO Devices

If you plan to use Cisco Network Services Orchestrator (Cisco NSO) as a provider to configure devices managed by Cisco Crosswork, be sure that the Cisco NSO device configurations observe the guidelines in the following example.

This example shows a Cisco NSO configuration that uses the hostname as the device ID. If you are using a CSV file to import devices, use **ROBOT_PROVDEVKEY_HOST_NAME** as the enum value for the provider_node_key field. The example hostname **RouterFremont** used here must match the hostname for the device in the CSV file.

```
configure
set devices device RouterFremont address 198.18.1.11 port 22
set devices device RouterSFO address 198.18.1.12 port 830
```

In the following example, we are creating an authgroup called "cisco", with a remote name and password of "cisco". Next, we are setting all the devices that have a name starting with "Router" to a device type of "netconf" using the ned-id "cisco-iosxr-nc-6.6". Finally, we are assigning all of the devices with a name starting with "Router" to the "cisco" authgroup. Edit these settings to match your environment:

```
set devices authgroups group cisco default-map remote-name cisco remote-password cisco
set devices device Router* device-type netconf ned-id cisco-iosxr-nc-6.6
set devices device Router* authgroup cisco
```

The following CLI commands unlock and retrieve the SSH keys from all of the devices. Cisco NSO synchronizes itself with the devices by uploading each device's current configuration and then storing the present configuration. It is important to use these commands to ensure that the devices, Cisco NSO, and your Cisco Crosswork applications are starting from a common configuration:

```
set devices device Router* state admin-state unlocked
request devices device Router* ssh fetch-host-keys
request devices device Router* sync-from
```

```
commit
```

Add Devices through the UI

Follow the steps below to add devices one by one, using the UI. Under normal circumstances, you will want to use this method only when adding a few devices.

Step 1 From the main menu, choose **Device Management** > **Network Devices**.

Step 2 Click ➕.

Step 3 Enter values for the new device, as listed in the table below.

Step 4 Click **Save**. The Save button is disabled until all mandatory fields are completed.

Step 5 (Optional) Repeat these steps to add more devices.

Table 1: Add New Device Window (=Required)*

Field	Description
*** Administration State**	The management state of the device. Options are • **UNMANAGED**—Crosswork is not monitoring the device. • **DOWN**—The device is being managed and is down. • **UP**—The device is being managed and is up.
*** Reachability Check**	Determines whether Crosswork performs reachability checks on the device. Options are: • **ENABLE** (In CSV: **REACH_CHECK_ENABLE**)—Checks for reachability and then updates the Reachability State in the UI automatically. • **DISABLE** (In CSV: **REACH_CHECK_DISABLE**)—The device reachability check is disabled. Cisco recommends that you always set this to **ENABLE**. This field is optional if **Configured State** is marked as **UNMANAGED**.
*** Credential Profile**	The name of the credential profile to be used to access the device for data collection and configuration changes. For example: **nso23** or **srpce123**. This field is optional if **Configured State** is marked as **UNMANAGED**.
Host Name	The host name of the device.
Inventory ID	Inventory ID value for the device. The value can contain a maximum of 128 alphanumeric characters, and can include dots (.), underscores ("_"), colons (":"), or hyphens ("-"). No other special characters are allowed. Choose the device Host Name or an easily identifiable name for Inventory ID as this will be used to sync the device to Crosswork with the Inventory ID used as the device name.
Software Type	Software type of the device.
Software Version	Software version of the device.

Field	Description
UUID	Universally unique identifier (UUID) for the device.
Serial Number	Serial number for the device.
MAC Address	MAC address of the device.
*** Capability**	The capabilities that allow collection of device data and that are configured on the device. You must select at least **`SNMP`** as this is a required capability. The device will not be onboarded if **`SNMP`** is not configured. Other options are **`YANG_MDT`**, **`YANG_CLI`**, **`TL1`**, and **`GNMI`**. The capabilities you select will depend on the device software type and version. **Note** • For devices with MDT capability, do not select **YANG_MDT** at this stage. • To enable Crosswork to receive the Syslog-based data, select **YANG_CLI**.
Tags	The available tags to assign to the device for identification and grouping purposes. Use device tags to group devices for monitoring, and to provide additional information that might be of interest to other users, such as the device's physical location or its administrator's email ID.
Product Type	Product type of the device.
Syslog Format	The format in which syslog events received from the device should be parsed by the Syslog Collector. The options are: • **`UNKNOWN`** - Choose this option if you are uncertain or if you do not want any parsing to be done by the Syslog Collector. The Syslog Collection Job output will contain syslog events as received from device. • **`RFC5424`** - Choose this option to parse syslog events received from the device in RFC5424 format. • **`RFC3164`** - Choose this option to parse syslog events received from the device in RFC5424 format. Refer to Section: Syslog Collection Job Output for more details.
Connectivity Details	
Protocol	The connectivity protocols used by the device. Choices are: **`SNMP`**, **`NETCONF`**, **`TELNET`**, **`HTTP`**, **`HTTPS`**, **`GNMI`**, **`TL1`**, and **`GRPC`**. **Note** Toggle the **Secure Connection** slider to secure the GNMI protocol that you have selected. To add more connectivity protocols for this device, click + at the end of the first row in the **Connectivity Details** panel. To delete a protocol you have entered, click × shown next to that row in the panel. You can enter as many sets of connectivity details as you want, including multiple sets for the same protocol. You must enter details for at least **`SSH`** and **`SNMP`**. If you do not configure **`SNMP`**, the device will not be added. If you want to manage the device (or you are managing XR devices), you must enter details for **`NETCONF`**. **`TELNET`** connectivity is optional.

Field	Description
*** IP Address / Subnet Mask**	Enter the device's IP address (IPv4 or IPv6) and subnet mask. **Note** Please ensure that the subnets chosen for the IP networks (including devices and destinations) do not have overlapping address space (subnets/supernets) as it may result in unpredictable connectivity issues. **Note** If you have multiple protocols with same IP address and subnet mask, you can instruct Crosswork to autofill the details in the other fields.
*** Port**	The port used for this connectivity protocol. Each protocol is mapped to a port, so be sure to enter the port number that corresponds to the **Protocol** you chose. The standard port assignments for each protocol are: • SSH: 22 • SNMP: 161 • NETCONF: 830 • TELNET: 23 • HTTP: 80 • HTTPS: 443 GNMI and GNMI_SECURE: The port values range between 57344 to 57999. Ensure that the port number you enter here matches with the port number configured on the device.
Timeout	The elapsed time (in seconds) before communication attempts using this protocol will time out. The default value is 30 seconds. For XE devices using NETCONF, the recommended minimum timeout value is 90 seconds. For all other devices and protocols, the recommended minimum timeout value is 60 seconds.
Encoding Type	This field is only applicable for **GNMI** and **GNMI_SECURE** protocols. The options are **`PROTO`** and **`JSON IETF`**. Based on device capability, only one encoding format is supported at a time in a device.
Encryption	This field is only applicable for **SNMP** protocol. From the drop-down menu, select the relevant SNPMv3 protocol supported by the device. The default value is NONE. The drop-down menu lists Advanced Encryption Standard (AES) specifications in Counter mode (CTR), Galois/Counter mode (GCM), and Cipher Block Chaining mode (CBC) for different key lengths (128-bit, 192-bit, 256-bit). The credential profile supports generic privacy types such as AES-192 and AES-256. In case of Cisco devices, AES-192 and AES-256 are customized as CiscoAES192 and CiscoAES256 protocols. On the devices, these protocols are displayed as aes256-ctr, aes256-gcm@openssh.com, aes256-cbc, aes192-ctr, and aes192-cbc. The Cisco devices will only respond to Crosswork's polling if it is based on the new protocol variations. For devices other than Cisco, select None in the **Encryption** field.

Field	Description
SNMP Disable Trap Check	This check box appears when the protocol field is set to `SNMP`. Selecting this check box, disables the SNMPv2 community string validation between the network device and Crosswork Data Gateway.
Routing Info	
ISIS System ID	The device's IS-IS system ID. This ID identifies the router in an IS-IS topology, and is required for SR-PCE integration.
OSPF Router ID	The device's OSPF router ID. This ID identifies the router in an OSPF topology, and is required for SR-PCE integration.
***TE Router ID**	The traffic engineering router ID for the respective IGP. **Note** For visualizing L3 links in topology, devices should be onboarded to Cisco Crosswork with the **TE Router ID** field populated.
IPv6 Router ID	IPv6 router ID for the device. This field is a configurable parameter, and cannot be autodiscovered by Crosswork.
Streaming Telemetry Config	
Vrf	Name of the VRF within which Model Driven Telemetry (MDT) traffic is routed.
Source Interface	The range of loopback in the device type. This field is optional. **Note** This field can be edited only when the device is in DOWN or UNMANAGED state.
Opt Out MDT Config	Enabling this checkbox skips Crosswork from pushing telemetry configuration to the device via NSO. The default setting state is Disabled (which allows Crosswork to push telemetry configuration to the device via NSO). The device must be in ADMIN DOWN state to toggle this setting. Any out of band configuration setup needs to be cleared before moving the setting from Enabled to Disabled.
Location All location fields are optional, with the exception of **Longitude** and **Latitude**, which are required for the geographical view of your network topology.	
Longitude, **Latitude**	Longitude and latitude values are required so that the geographical map can present the correct geographical location of the device and its links to other devices. Enter the longitude and latitude in Decimal Degrees (DD) format.
Altitude	The altitude, in feet or meters, at which the device is located. For example, `123`.
Providers and Access To add more providers for this device, click + at the end of the first row in the **Providers and Access** panel. To delete a provider you have entered, click × shown next to that row in the panel.	
Provider Family	Provider type used for topology computation. Choose a provider from the list.

Field	Description
Provider Name	Provider name used for topology computation. Choose a provider from the list. **Note** For Cisco NSO LSA deployment, the user can select the resource-facing service (RFS) node to which they want to assign the device.
Credential	The Credential profile used for the provider. This field is read-only and is autopopulated based on the provider you select.

Add Devices by Importing from CSV File

Complete the steps below to create a CSV file that specifies multiple devices and then import it into Crosswork.

Importing devices from a CSV file adds any devices not already in the database, and overwrites the data in any device record with an Inventory Key Type field value that matches those of an imported device (this excludes the UUID, which is set by the system and not affected by import). For this reason, it is a good idea to export a backup copy of all your current devices before an import.

Attention

- While importing a large number of devices via a CSV file, value for the **TE Router ID** field should be populated.
- Importing large number of devices with incorrect CSV values using a Firefox browser may render the window unusable. If this happens, log in to Cisco Crosswork in a new tab or window, and onboard devices with correct CSV values.
- The CSV files created on a Windows machine should contain a newline (marked with a 'newline' character) for the file to be processed as expected. Any newline created using the "carriage return" option will not work.

Step 1 From the main menu, choose **Device Management** > **Network Devices**. The **Network Devices** tab is displayed by default.

Step 2 Click to open the **Import CSV File** dialog box.

Step 3 If you have not already created a device CSV file to import:

a) Click the **Download sample 'Device Management template (*.csv)' file** link and save the CSV file template to a local storage resource.

b) Open the template using your preferred tool. Begin adding rows to the file, one row for each device.

Note

- Confirm that the TE router ID value for each device is populated. This value is used to uniquely identify the device in the topology which is learned from SR-PCE. Without a valid TE router ID for each device, the topology will not be displayed.
- After importing a device or onboarding a device, the TE Router ID should not be changed. If it is necessary to change the TE Router ID of a device after it has been imported then do the following:
    1. The device should be removed from Crosswork.
    2. All SR-PCE Providers should be removed.
    3. Onboard the device again with the new TE Router ID.
    4. Add the SR-PCE providers again.

Use a semicolon to separate multiple entries in the same field. Use two semicolons with no space between them to indicate that you are leaving the field blank. When you separate multiple entries with semicolons, remember that the order in which you enter values in each field is important. For example, if you enter `SSH;SNMP;NETCONF` in the **Connectivity Type** field and you enter `22;161;830` in the **Connectivity Port** field, the order of entry determines the mapping between the two fields:

- SSH: port 22
- SNMP: port 161
- NETCONF: port 830

For a list of the fields and the mandatory values you must enter, see the "Add New Device" field table in Add Devices through the UI, on page 8.

Be sure to delete the sample data rows before saving the file, or they will be imported along with the data you want. The column header row can stay, as it is ignored during import.

c) When you are finished, save the new CSV file.

Step 4 Click **Browse** to navigate to the CSV file you created in the previous steps and then click **Open** to select it.

Step 5 With the CSV file selected, click **Import**.

Note While importing devices or providers via UI using a CSV file, the user should wait for the operation to complete. Clicking the **Import** button while the operation is in progress will lead to duplicate entries for each device or provider.

Step 6 Resolve any errors and confirm device reachability.

It is normal for devices to show as unreachable or not operational when they are first imported. However, if they are still displayed as unreachable or not operational after 30 minutes, there may be an issue that needs to be investigated. To investigate, select **Device Management** > **Job History** and click on any error icon you see in the **Status** column. Common issues include failure to ensure the associated credential profile contains the correct credentials. You can test this by opening a terminal window on the server and then trying to access the device using the protocol and credentials specified in the associated credential profile.

Step 7 Once you have successfully on boarded the devices, you must map them to a Cisco Crosswork Data Gateway instance.

Export Device Information to a CSV File

When you export the device list, all device information is exported to a CSV file. Exporting the device list is a handy way to keep a record of all devices in the system at one time. You can also edit the CSV file as needed, and re-import it to overwrite existing device data.

The exported device CSV file will contain only the name of the credential profile for each device, not the credentials themselves.

Step 1 From the main menu, choose **Device Management** > **Network Devices**. The **Network Devices** tab is displayed by default.

Step 2 (Optional) Filter the device list as needed.

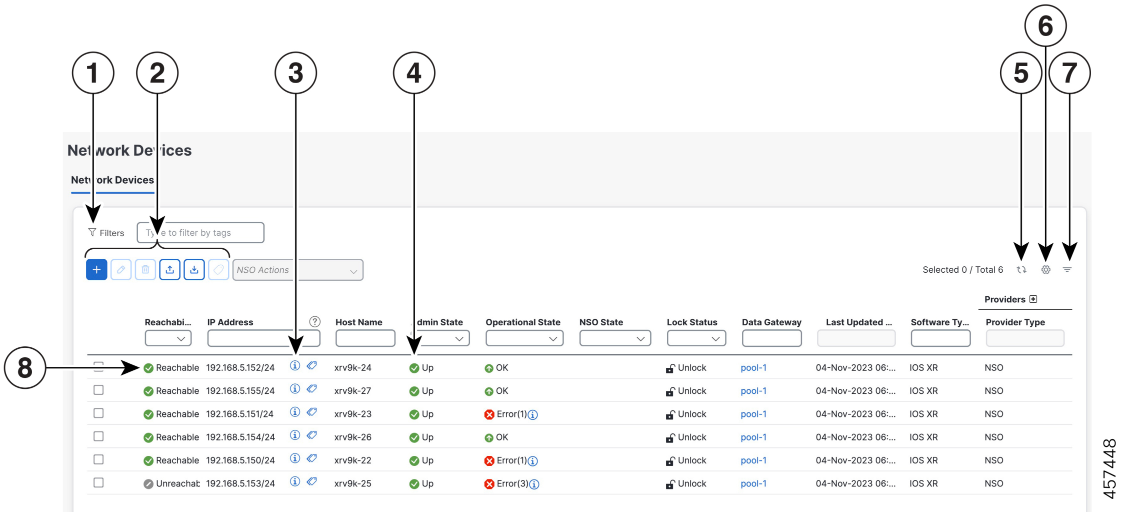
Step 3 Check the check boxes for the devices you want to export. Check the check box at the top of the column to select all the devices for export.

Step 4 Click the ⇪. Your browser will prompt you to select a path and the file name to use when saving the CSV file, or to open it immediately

Manage Network Devices

Cisco Crosswork's **Network Devices** window gives you a consolidated list of all your devices and their status. To view the **Network Devices** window, select **Device Management** > **Network Devices**. The **Network Devices** tab is displayed by default.

Figure 1: Network Devices Window



	Reachabi...	IP Address	?	Host Name	dmin State	Operational State	NSO State	Lock Status	Data Gateway	Last Updated ...	Software Ty...	Provider Type
□	Reachable	192.168.5.152/24	ⓘ	xrv9k-24	Up	OK		Unlock	pool-1	04-Nov-2023 06:...	IOS XR	NSO
□	Reachable	192.168.5.155/24	ⓘ	xrv9k-27	Up	OK		Unlock	pool-1	04-Nov-2023 06:...	IOS XR	NSO
□	Reachable	192.168.5.151/24	ⓘ	xrv9k-23	Up	Error(1)ⓘ		Unlock	pool-1	04-Nov-2023 06:...	IOS XR	NSO
□	Reachable	192.168.5.154/24	ⓘ	xrv9k-26	Up	OK		Unlock	pool-1	04-Nov-2023 06:...	IOS XR	NSO
□	Reachable	192.168.5.150/24	ⓘ	xrv9k-22	Up	Error(1)ⓘ		Unlock	pool-1	04-Nov-2023 06:...	IOS XR	NSO
□	Unreachat	192.168.5.153/24	ⓘ	xrv9k-25	Up	Error(3)ⓘ		Unlock	pool-1	04-Nov-2023 06:...	IOS XR	NSO

Item	Description
1	The **Filter by tags** field lets you filter the devices by the tags applied to them. Type the name of the tag that has been applied to the device that you are trying to find.

Item	Description
2	Click the + to add a new device to the device inventory.
	Click the ✎ to edit the information for the currently selected devices. .
	Click the 🗑 to delete the currently selected devices.
	Click the ⤓ to import new devices and update existing devices, using a CSV file. You can also download a CSV file template by clicking this icon. The template includes sample data that you can use as a guide for building your own CSV file.
	Click the ⤒ to export information for selected devices to a CSV file.
	Click the 🏷 to modify tags applied to the selected devices. See .
3	Click the ⓘ to open the **Device Details** pop-up window, where you can view important information for the selected device.
4	Icons in the **Administration State** column show whether a device is operational or not.
5	Click the ⟳ to refresh the Devices list.
6	Click the ⚙ to select which columns to display in the Devices list.
7	Click ≡ to set filter criteria on one or more columns in the Devices list.
	Click the **Clear Filter** link to clear any filter criteria you may have set.
8	Icons in the **Reachability State** column show whether a device is reachable or not.

Device State

Cisco Crosswork computes the Reachability State of the providers it uses and devices it manages, as well as the Operational and NSO States of reachable managed devices. It indicates these states using the icons in the following table.

Table 2: Device State Icons

This Icon...	Indicates...
Reachability State icons show whether a device or a provider is reachable or not	
✓	Reachable: The device or provider can be reached by all configured protocols configured fo
↻	Reachability Degraded: The device or provider can be reached by at least one protocol, but configured for it.
✖	Unreachable: The device or provider cannot be reached by reachable by any protocol confi

This Icon...	Indicates...
?	Reachability Unknown: Cisco Crosswork cannot determine if the device is reachable, degraded, is not connected to Cisco Crosswork Data Gateway.
Operational State icons show whether a device is operational or not.	
⬆	The device is operational and under management, and all individual protocols are "OK" (also l
⬇	The device is not operational ("down"). The same icon is used when the device has been set "ad
?	The device's operational or configuration state is unknown.
~	The device's operational or configuration state is degraded.
✖①	The device's operational or configuration state is in an error condition. It is either not up, or unr attempting to reach it and compute its operational state. The number in the circle shown next to on the number to see a list of these errors. (Note that the icon badging for errors is not available
…	The device's operational state is currently being checked.
✖	The device is being deleted.
⊖	The device is unmanaged.
NSO State icons show whether a device is synced with Cisco NSO or not. **Note** In the initial sync between Cisco Crosswork and NSO after onboarding a device, the NSO state column in t Crosswork has not determined if the device needs to sync with NSO based on the policy, and cannot select t	
✓	The device is in sync with Cisco NSO.
!	The device is out of sync with Cisco NSO.

The Reachability State of a device is computed as follows:

1. Reachability is always computed for each device as long as the device's configured state (as configured by users) is UP. It is not computed if the device is administratively DOWN or UNMANAGED.
2. Reachability state is always either REACHABLE, UNREACHABLE, or UNKNOWN.
    - The Reachability state is REACHABLE if there is at least one route to the device via at least one protocol AND the device is discoverable.
    - The Reachability state is UNREACHABLE if there are no routes to the device via one protocol OR the device does not respond.
    - The Reachability state is UNKNOWN if the device is UNMANAGED.

The Operational State of a device is computed as follows:

1. Operational state is always computed for each device as long as the device's configured state (as configured by users) is UP. It is not computed if the device is administratively DOWN or UNMANAGED.
2. Operational state is always OK or ERROR.
3. For a device to be Operational=OK, the device must be REACHABLE and discoverable. Any other Reachability state is ERROR.
4. For XR or XE devices only, Operational=OK also requires that Clock Drift difference between the Crosswork host and device clocks is <=the default Drift Value, currently 2 minutes.

Note Some timezone settings are known to result in Clock Drift errors when no clock drift actually exists. To work around this issue set your devices to use UTC time.

Filter Network Devices by Tags

By creating a tag and assigning it to a particular device, you can easily provide additional information that might be of interest to other users, such as the device’s physical location and its administrator’s email ID. You can also use tags to find and group devices with the same or similar tags in any window that lists devices.

To filter devices by tags:

Step 1 From the main menu, choose **Device Management** > **Network Devices**.

Step 2 In the **Type to filter by tags** bar at the top of the user interface, type all or part of the name of a tag.

The **Type to filter by Tags** bar has a type-ahead feature: As you start typing, the field shows a drop-down list of tags that match all the characters you have typed so far. To force the drop-down list to display all available tags, type *.

Step 3 Choose the name of the tag you want to add to the filter. The filter appears in the **Type to filter by tags** filter bar. The table or map shows only the devices with that tag.

Step 4 If you want to filter on more than one tag:

a) Repeat Steps 2 and 3 for each additional tag you want to set as part of the filter.

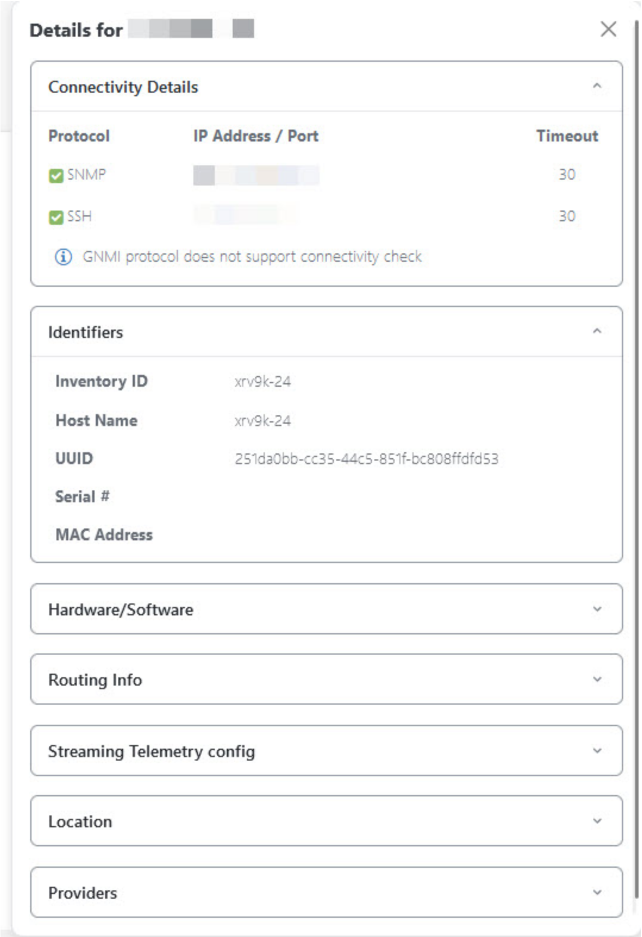
b) When you have selected all the tags you want, click **Apply Filters**. The table or map shows only the devices with tags that match **all** the tags in your filter.

Step 5 To clear all tag filters, click the **Clear Filters** link. To remove a tag from a filter containing multiple tags, click the **X** icon next to that tag's name in the filter.

Get More Information About a Device

Whenever you select **Device Management** > **Network Devices** and display the list of devices under the **Network Devices** tab, you can click the ⓘ next to any listed device to get more information about that device. Clicking this icon opens the **Details for DeviceName** pop-up window, as shown in the following example:

Figure 2: Details for DeviceName Window



Details for [redacted]

Connectivity Details

Protocol	IP Address / Port	Timeout
☑ SNMP	[redacted]	30
☑ SSH	[redacted]	30

GNMI protocol does not support connectivity check

Identifiers

Inventory ID	xrv9k-24
Host Name	xrv9k-24
UUID	251da0bb-cc35-44c5-851f-bc808ffdfd53
Serial #	
MAC Address	

Expand the **Connectivity Details** area at the top of the pop-up window (if it is not already expanded). This area shows the reachability status for all transport types.

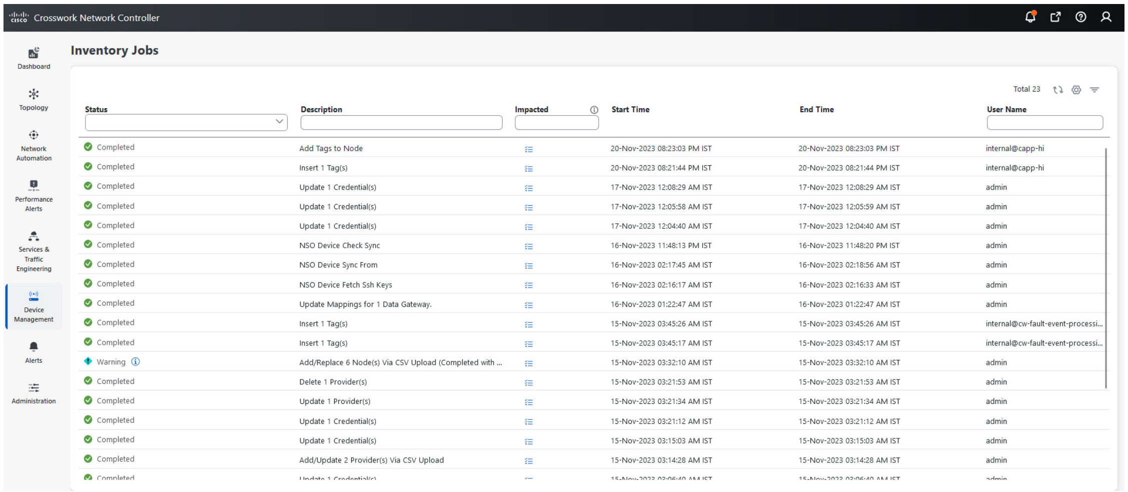
Expand and collapse the other areas of the pop-up window, as needed. Click the ✕ to close the window.

View Device Job History

Cisco Crosswork collects and stores information about device-related jobs. Follow the steps below to track all create, update and delete activities.

Step 1 From the main menu, choose **Device Management** > **Inventory Jobs**. The **Inventory Jobs** window opens displaying a log of all device-related jobs, like the one shown below.

Figure 3: Inventory Jobs window



Inventory Jobs

Status	Description	Impacted	Start Time	End Time	User Name
Completed	Add Tags to Node	☰	20-Nov-2023 08:23:03 PM IST	20-Nov-2023 08:23:03 PM IST	internal@capp-hi
Completed	Insert 1 Tag(s)	☰	20-Nov-2023 08:21:44 PM IST	20-Nov-2023 08:21:44 PM IST	internal@capp-hi
Completed	Update 1 Credential(s)	☰	17-Nov-2023 12:08:29 AM IST	17-Nov-2023 12:08:29 AM IST	admin
Completed	Update 1 Credential(s)	☰	17-Nov-2023 12:05:58 AM IST	17-Nov-2023 12:05:59 AM IST	admin
Completed	Update 1 Credential(s)	☰	17-Nov-2023 12:04:40 AM IST	17-Nov-2023 12:04:40 AM IST	admin
Completed	NSO Device Check Sync	☰	16-Nov-2023 11:48:13 PM IST	16-Nov-2023 11:48:20 PM IST	admin
Completed	NSO Device Sync From	☰	16-Nov-2023 02:17:45 AM IST	16-Nov-2023 02:18:56 AM IST	admin
Completed	NSO Device Fetch Ssh Keys	☰	16-Nov-2023 02:16:17 AM IST	16-Nov-2023 02:16:33 AM IST	admin
Completed	Update Mappings for 1 Data Gateway.	☰	16-Nov-2023 01:22:47 AM IST	16-Nov-2023 01:22:47 AM IST	admin
Completed	Insert 1 Tag(s)	☰	15-Nov-2023 03:45:26 AM IST	15-Nov-2023 03:45:26 AM IST	internal@cw-fault-event-processi...
Completed	Insert 1 Tag(s)	☰	15-Nov-2023 03:45:17 AM IST	15-Nov-2023 03:45:17 AM IST	internal@cw-fault-event-processi...
Warning ⓘ	Add/Replace 6 Node(s) Via CSV Upload (Completed with ...	☰	15-Nov-2023 03:32:10 AM IST	15-Nov-2023 03:32:10 AM IST	admin
Completed	Delete 1 Provider(s)	☰	15-Nov-2023 03:21:53 AM IST	15-Nov-2023 03:21:53 AM IST	admin
Completed	Update 1 Provider(s)	☰	15-Nov-2023 03:21:34 AM IST	15-Nov-2023 03:21:34 AM IST	admin
Completed	Update 1 Credential(s)	☰	15-Nov-2023 03:21:12 AM IST	15-Nov-2023 03:21:12 AM IST	admin
Completed	Update 1 Credential(s)	☰	15-Nov-2023 03:15:03 AM IST	15-Nov-2023 03:15:03 AM IST	admin
Completed	Add/Update 2 Provider(s) Via CSV Upload	☰	15-Nov-2023 03:14:28 AM IST	15-Nov-2023 03:14:28 AM IST	admin
Completed	Update 1 Credential(s)	☰	15-Nov-2023 03:06:40 AM IST	15-Nov-2023 03:06:40 AM IST	admin

The jobs display in descending order of creation time. The most recent job is shown first. To sort the data in the table, click a column heading. Click the column heading again to toggle between ascending and descending sort order.

Step 2 The **Status** column shows the types of states: completed, failed, running, partial, and warning. For any failed or partial job, click the ⓘ shown next to the error for more information.

Note The status may be displayed as **Successful** even when the device is not reachable. You can verify that the status of the jobs that is displayed is correct by also looking into the status of the device (**Device Management** > **Network Devices**).

Edit Devices

Complete the following procedure to update a device's information.

Before editing any device, it is always good practice to export a CSV backup of the devices you want to change.

Step 1 From the main menu, choose **Device Management** > **Network Devices**.

Step 2 (Optional) Filter the list of devices by filtering specific columns.

Step 3 Check the check box of the device you want to change, then click the ✎.

Step 4 Edit the values configured for the device, as needed.

Note User-configured parameters like ISIS System ID and OSPF Router ID are not auto-discovered by Crosswork device management for onboarded devices. These fields may appear blank when you edit the device, however, the topology page for the same device will display the parameters.

Note In addition to the existing fields, you can also view the **Data Gateway** configured for the selected device. This field is read-only.

Step 5 Click **Save**. The Save button remains dimmed until all required fields are completed.

Step 6 Resolve any errors and confirm device reachability.

Delete Devices

Complete the following procedure to delete devices.

Before you begin

- If you set the **`auto-onboard`** property as **managed** or **unmanaged** for an SR-PCE provider, set **`auto-onboard`** as **off** for one or more SR-PCEs.
- Confirm that the device is disconnected and powered off before deleting the device.
- If devices are mapped to Cisco NSO with MDT capability, and telemetry configuration is pushed, then those configurations will be removed from the device.
- If **`auto-onboard`** is not **off** and it is still functional and connected to the network, the device will be rediscovered as unmanaged when it is deleted.

Step 1 Export a backup CSV file containing the devices that you plan to delete.

Step 2 From the main menu, choose **Device Management** > **Network Devices**.

Step 3 (Optional) In the **Devices** window, filter the list of devices by entering text in the **Search** field or filtering specific columns.

Step 4 Check the check boxes for the devices you want to delete.

Step 5 Click the 🗑.

Step 6 In the confirmation dialog box, click **Delete**.

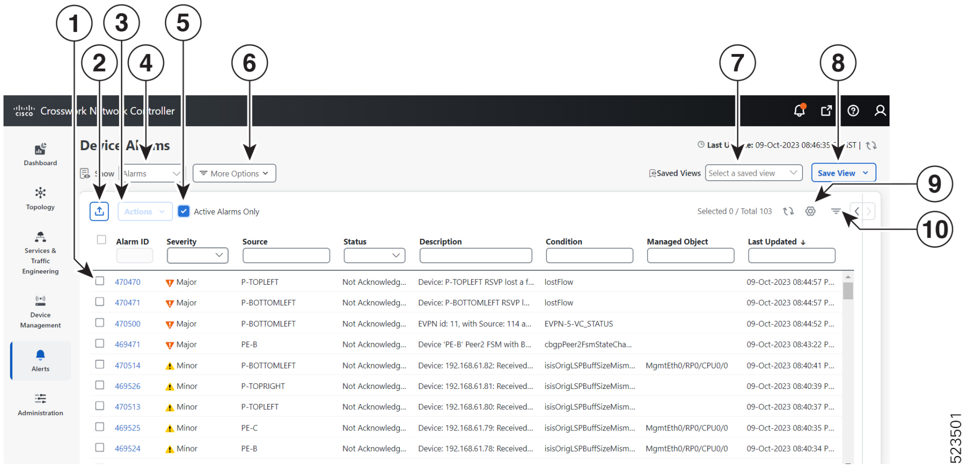
Work With Device Alerts

Cisco Crosswork refers to device alarms and events as "alerts". The **Device Alarms** and **Device Events** windows give you a consolidated list of all alerts for your devices. You can toggle between the **Device Alarms** and **Device Events** windows using the **Show** option on each window.

To view the **Device Alarms** window, select **Alerts** > **Device Alarms**. By default, Crosswork displays the **Device Alarms** window with the **Show** selection set to **Alarms**, as shown in the first figure below.

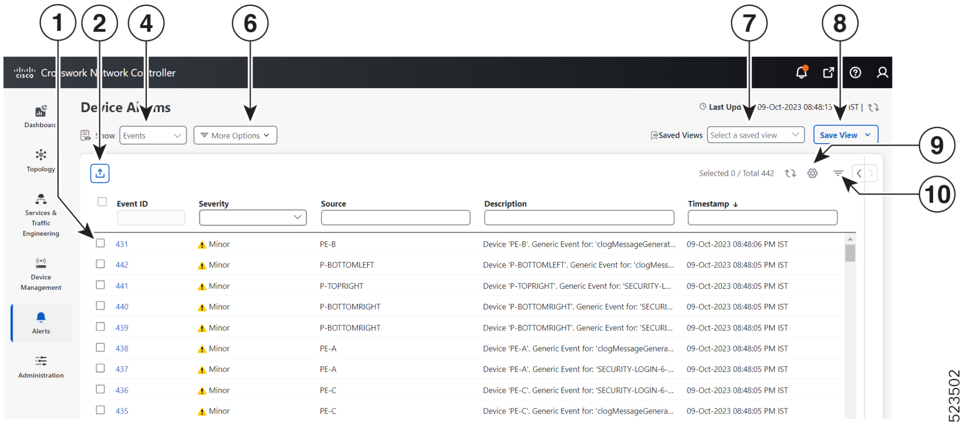
To view the **Device Events** window, first select **Alerts** > **Device Alarms**. Then change the **Show** selection to **Events**. Crosswork displays the **Device Events**window, as shown in the second figure below.

Figure 4: Device Alarms Window



□	Alarm ID	Severity	Source	Status	Description	Condition	Managed Object	Last Updated ↓
□	470470	Major	P-TOPLEFT	Not Acknowledg...	Device: P-TOPLEFT RSVP lost a f...	lostFlow		09-Oct-2023 08:44:57 P...
□	470471	Major	P-BOTTOMLEFT	Not Acknowledg...	Device: P-BOTTOMLEFT RSVP l...	lostFlow		09-Oct-2023 08:44:57 P...
□	470500	Major	P-BOTTOMLEFT	Not Acknowledg...	EVPN id: 11, with Source: 114 a...	EVPN-5-VC_STATUS		09-Oct-2023 08:44:52 P...
□	469471	Major	PE-B	Not Acknowledg...	Device 'PE-B' Peer2 FSM with B...	cbgpPeer2FsmStateCha...		09-Oct-2023 08:43:22 P...
□	470514	Minor	P-BOTTOMLEFT	Not Acknowledg...	Device: 192.168.61.82: Received...	isisOrigLSPBuffSizeMism...	MgmtEth0/RP0/CPU0/0	09-Oct-2023 08:40:41 P...
□	469526	Minor	P-TOPRIGHT	Not Acknowledg...	Device: 192.168.61.81: Received...	isisOrigLSPBuffSizeMism...		09-Oct-2023 08:40:39 P...
□	470513	Minor	P-TOPLEFT	Not Acknowledg...	Device: 192.168.61.80: Received...	isisOrigLSPBuffSizeMism...		09-Oct-2023 08:40:37 P...
□	469525	Minor	PE-C	Not Acknowledg...	Device: 192.168.61.79: Received...	isisOrigLSPBuffSizeMism...	MgmtEth0/RP0/CPU0/0	09-Oct-2023 08:40:35 P...
□	469524	Minor	PE-B	Not Acknowledg...	Device: 192.168.61.78: Received...	isisOrigLSPBuffSizeMism...	MgmtEth0/RP0/CPU0/0	09-Oct-2023 08:40:34 P...

Figure 5: Device Events Window



□	Event ID	Severity	Source	Description	Timestamp ↓
□	431	Minor	PE-B	Device 'PE-B'. Generic Event for: 'clogMessageGenerat...	09-Oct-2023 08:48:06 PM IST
□	442	Minor	P-BOTTOMLEFT	Device 'P-BOTTOMLEFT'. Generic Event for: 'clogMess...	09-Oct-2023 08:48:05 PM IST
□	441	Minor	P-TOPRIGHT	Device 'P-TOPRIGHT'. Generic Event for: 'SECURITY-L...	09-Oct-2023 08:48:05 PM IST
□	440	Minor	P-BOTTOMRIGHT	Device 'P-BOTTOMRIGHT'. Generic Event for: 'SECURI...	09-Oct-2023 08:48:05 PM IST
□	439	Minor	P-BOTTOMRIGHT	Device 'P-BOTTOMRIGHT'. Generic Event for: 'SECURI...	09-Oct-2023 08:48:05 PM IST
□	438	Minor	PE-A	Device 'PE-A'. Generic Event for: 'clogMessageGenera...	09-Oct-2023 08:48:05 PM IST
□	437	Minor	PE-A	Device 'PE-A'. Generic Event for: 'SECURITY-LOGIN-6-...	09-Oct-2023 08:48:05 PM IST
□	436	Minor	PE-C	Device 'PE-C'. Generic Event for: 'SECURITY-LOGIN-6-...	09-Oct-2023 08:48:05 PM IST
□	435	Minor	PE-C	Device 'PE-C'. Generic Event for: 'clogMessageGenera...	09-Oct-2023 08:48:05 PM IST

Item	Description
1	Click the selection box next to the **Alarm ID** or **Event ID**column to select one or more alerts. Click the blue ID link in the **Alarm ID** or **Event ID**column to view details for that alert. See View Alert Details, on page 23 for more information. On the **Device Alarms** window only: When you have one or more alarms selected, Crosswork enables the **Actions** menu, so you can acknowledge, clear or annotate the selected alarms.
2	Click the ⇪ icon to export a PDF or CSV file listing full information for all the alerts shown in the window. If you have one or more alerts selected at the time you click the icon, the file will contain information for the selected alerts only. See Export Alerts, on page 27 for more information.

Item	Description
3	On the **Device Alarms** window only: Click the **Actions** dropdown menu to perform one or more of these actions on the currently selected alarms: • **Acknowledge**: Marks the currently selected alarms as acknowledged. See Acknowledge Alarms, on page 24 for more information. • **Unacknowledge**: If any of the currently selected alarms have been acknowledged, restores them to the unacknowledged state. • **Clear**: Removes all currently selected alarms from the **Device Alarms** window. See Clear Alarms, on page 25 for more information. • **Clear all of this condition**: Removes all currently selected alarms that share the same condition. • **Notes**: Lets you add a text note to all of the currently selected alarms. See Annotate Alarms, on page 25 for more information. Crosswork enables the **Actions** menu only until you select one or more alarms using the selection box next to the **Alarm ID** column.
4	Toggles between the **Device Alarms** and **Device Events** windows.
5	On the **Device Alarms** window only: Move the slider to set the window to display **All Alarms** or **Active Alarms only**. The default is **Active Alarms only**.
6	Click on **More Options** to specify whether you want to view all alerts or only the latest, and how often to sync the alerts display with the Crosswork database. If you uncheck the **Alarm History** or **Event History** checkbox, the list shows all alerts. If you uncheck the **Auto Sync** checkbox, Crosswork pauses synchronization.
7	Click in the **Saved Views** field to manage the previously saved views created using the **Save View** button. The popup **Manage Saved Views** window allows you to view, sort, see all views or only those you have saved. See Work With Saved Alert Views, on page 26 for more information.
8	Click the **Save View** button to save the current view. Crosswork will prompt you to enter and save the view under a unique name.
9	Click the ⚙ to select which columns to display in the alerts list.
10	Click the ☰ to toggle display of the floating filter fields at the top of the alerts list. You can use these fields to set filter criteria on one or more columns in the list. Click the **Filters Applied** link, shown next to the icon, to clear any filter criteria you have set.

Crosswork lets you customize the alert settings to suit your production requirements. Click on the below topics for more information:

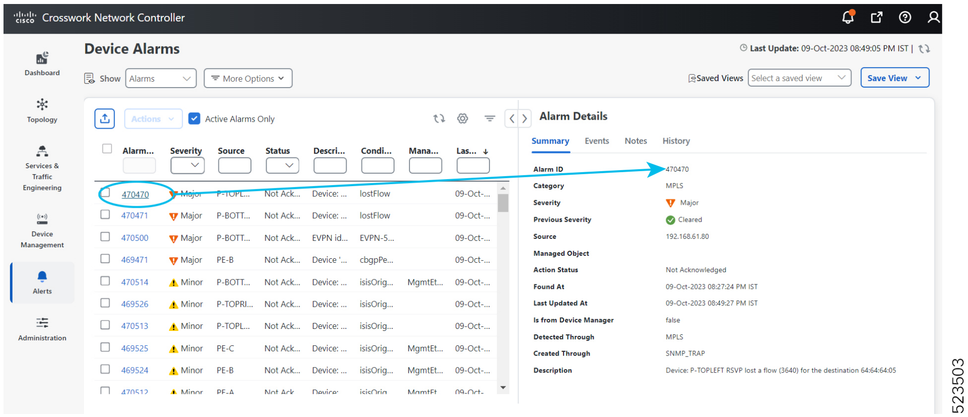
- Customize Alerting Devices, on page 27
- Customize Alarm Auto Clear, on page 28
- Customize Instructive Text for Alarms, on page 28
- Customize Alert Cleanup, on page 29
- Customize Alarm Severity, on page 30

View Alert Details

Whenever you select **Alerts** > **Device Alerts** and display the list of alarms or events, you can click the ID number for any alert in the **Alarm ID** or **Event ID** column to get more information about that alert.

For example: If you select **Alerts** > **Device Alerts** to display the **Device Alarms** window, clicking on an ID number in the **Alarm ID** column opens an **Alarm Details** window like the one shown in the illustration below:

Figure 6: Alarm Details Window: Summary Tab



Device Alarms

Last Update: 09-Oct-2023 08:49:05 PM IST |

☑ Active Alarms Only

Alarm...	Severity	Source	Status	Descri...	Condi...	Mana...	Las...
470470	Major	P-TOPL...	Not Ack...	Device: ...	lostFlow		09-Oct-...
470471	Major	P-BOTT...	Not Ack...	Device: ...	lostFlow		09-Oct-...
470500	Major	P-BOTT...	Not Ack...	EVPN id...	EVPN-5...		09-Oct-...
469471	Major	PE-B	Not Ack...	Device '...	cbgpPe...		09-Oct-...
470514	Minor	P-BOTT...	Not Ack...	Device: ...	isisOrig...	MgmtEt...	09-Oct-...
469526	Minor	P-TOPRI...	Not Ack...	Device: ...	isisOrig...		09-Oct-...
470513	Minor	P-TOPL...	Not Ack...	Device: ...	isisOrig...		09-Oct-...
469525	Minor	PE-C	Not Ack...	Device: ...	isisOrig...	MgmtEt...	09-Oct-...
469524	Minor	PE-B	Not Ack...	Device: ...	isisOrig...	MgmtEt...	09-Oct-...
470512	Minor	PE-A	Not Ack	Device:	isisOrig	MgmtEt	09-Oct-

Alarm Details

Summary | Events | Notes | History

Alarm ID	470470
Category	MPLS
Severity	Major
Previous Severity	Cleared
Source	192.168.61.80
Managed Object	
Action Status	Not Acknowledged
Found At	09-Oct-2023 08:27:24 PM IST
Last Updated At	09-Oct-2023 08:49:27 PM IST
Is from Device Manager	false
Detected Through	MPLS
Created Through	SNMP_TRAP
Description	Device: P-TOPLEFT RSVP lost a flow (3640) for the destination 64:64:64:05

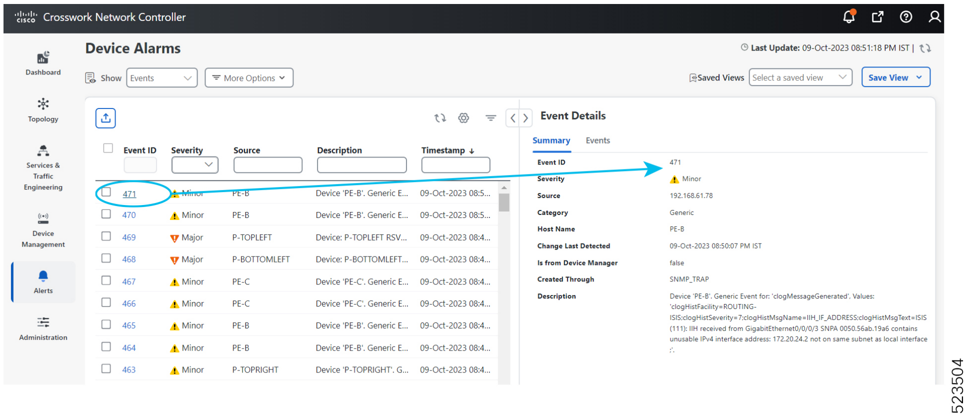
The **Summary** tab is the default, showing basic information about the alarm you selected.

While viewing the **Alarm Details** window, you can click on:

- The ⓘ next to the **Condition** field on the **Summary** tab. If customized for your organization, this displays a description of the condition and the action your organization recommends that you take to clear the alarm.
- The **Events** tab to see correlated events for the alarm you selected.
- The **Notes** tab to view annotations you or your colleagues have added to the alarm.
- The **History** tab to see information about when and how the alarm was raised and resolved.

You can do the same thing with events. For example: If you select **Alerts** > **Device Alerts** and then select **Events** in the **Show** field, Crosswork displays the **Device Events** window. If you then click on an ID number in the **Event ID** column, Crosswork displays an **Event Details** window like the one shown below:

Figure 7: Event Details Window: Summary Tab



Device Alarms

Last Update: 09-Oct-2023 08:51:18 PM IST |

	Event ID	Severity	Source	Description	Timestamp ↓
□	471	Minor	PE-B	Device 'PE-B'. Generic E...	09-Oct-2023 08:5...
□	470	Minor	PE-B	Device 'PE-B'. Generic E...	09-Oct-2023 08:5...
□	469	Major	P-TOPLEFT	Device: P-TOPLEFT RSV...	09-Oct-2023 08:4...
□	468	Major	P-BOTTOMLEFT	Device: P-BOTTOMLEFT...	09-Oct-2023 08:4...
□	467	Minor	PE-C	Device 'PE-C'. Generic E...	09-Oct-2023 08:4...
□	466	Minor	PE-C	Device 'PE-C'. Generic E...	09-Oct-2023 08:4...
□	465	Minor	PE-B	Device 'PE-B'. Generic E...	09-Oct-2023 08:4...
□	464	Minor	PE-B	Device 'PE-B'. Generic E...	09-Oct-2023 08:4...
□	463	Minor	P-TOPRIGHT	Device 'P-TOPRIGHT'. G...	09-Oct-2023 08:4...

Event Details

Event ID	471
Severity	Minor
Source	192.168.61.78
Category	Generic
Host Name	PE-B
Change Last Detected	09-Oct-2023 08:50:07 PM IST
Is from Device Manager	false
Created Through	SNMP_TRAP
Description	Device 'PE-B'. Generic Event for: 'clogMessageGenerated', Values: 'clogHistFacility=ROUTING-ISIS;clogHistSeverity=7;clogHistMsgName=IIH_IF_ADDRESS;clogHistMsgText=ISIS (111): IIH received from GigabitEthernet0/0/0/3 SNPA 0050.56ab.19a6 contains unusable IPv4 interface address: 172.20.24.2 not on same subnet as local interface ;'.

The **Event Details** window's **Summary** tab is the default, showing basic information about the event you selected.

While viewing the **Event Details** window, you can click on the **Events** tab to see other events correlated with the event you selected.

Acknowledge Alarms

Follow these steps to acknowledge device alarms, or return acknowledged alarms back to unacknowledged status. You can acknowledge multiple alarms at the same time by selecting their check boxes before selecting **Actions** > **Acknowledge** .

Acknowledging an alarm clears it permanently, but the alarm will still be listed in the **Device Alarms** window.

Step 1 From the main menu, choose **Device Alerts** > **Device Alarms** . Crosswork displays the **Device Alarms** window.

Step 2 (Optional) Filter the list of alarms by filtering columns, changing the **Active Alarms Only** slider, or adding or removing columns using the ⚙

Step 3 (Optional) Filter the list of alarms by filtering columns, or by adding or removing columns using the ⚙ and then filtering again. Use the **More Options** dropdown to choose whether you want to see only current alarms, and how often the window syncs the displayed list with the Crosswork database. Move the **Active Alarms Only** slider to show all alarms.

Step 4 Check the check box next to the ID of the alarm(s) you want to acknowledge.

Step 5 Select **Actions** > **Acknowledge**.

Step 6 Click **OK** to complete the acknowledgment action.

Step 7 To return an acknowledged alarm to the unacknowledged status:

a) Check the check box next to the ID of an acknowledged alarm.

b) Select **Actions** > **Unacknowledged**. Crosswork resets the alarm status to unacknowledged.

Clear Alarms

Follow these steps to clear device alarms. You can clear one or multiple alarms by selecting their check boxes. You can also choose to clear all alarms reporting the same alarm condition (such as "lostFlow" or "mplsTunnelDown").

Clearing an alarm removes it from the **Device Alarms** window, but the alarm will be generated again if the triggering event recurs.

Step 1 From the main menu, choose **Device Alerts** > **Device Alarms** . Crosswork displays the **Device Alarms** window.

Step 2 (Optional) Filter the list of alarms by filtering columns, changing the **Active Alarms Only** slider to show all alarms, or by adding or removing columns using the ⚙. Use the **More Options** dropdown to choose whether you want to see only current alarms or all alarms, and how often the window syncs the displayed list with the Crosswork database.

Step 3 Check the check box next to the ID of the alarm(s) you want to clear, then select **Actions** > **Clear**.

Step 4 Click **OK** to complete the clear action.

Step 5 To clear all alarms sharing the same condition:

a) Check the check box next to the ID of one or more alarms sharing the conditions you want to clear (you may select alarms with different conditions).

b) Select **Actions** > **Clear all of this condition**.

c) Click **OK** to complete the clear-all action.

Annotate Alarms

Alarm notes are a handy way to share information with colleagues and record important information missed by automated monitoring. Notes are permanently attached to the alarm and are retrievable until the alarm is cleared from the database or deleted by a user. The user ID of the note taker is stored with the note.

Follow the steps below to annotate device alarms. You can annotate multiple alarms at the same time by selecting their check boxes before choosing to add a note. Notes support entries in plain text only.

Step 1 From the main menu, choose **Device Alerts** > **Device Alarms** . Crosswork displays the **Device Alarms** window.

Step 2 (Optional) Filter the list of alarms by filtering columns, changing the **Active Alarms Only** slider to show all alarms, or by adding or removing columns using the ⚙. Use the **More Options** dropdown to choose whether you want to see only current alarms or all alarms, and how often the window syncs the displayed list with the Crosswork database.

Step 3 Check the check box next to the ID of the alarm(s) you want to annotate.

Step 4 Select **Actions** > **Notes**. Crosswork displays the **Add annotation** popup.

Step 5 Enter the text of the note you want to add to the selected alarm(s).

Step 6 Click **Add** to add the note.

Work With Saved Alert Views

You can use the filtering options on the **Device Alarms** and **Device Events** windows to show only the alerts you want. You can then save this filtered display as a saved view. You and other Crosswork users can recall the saved view to the window with a few clicks.

Note that individual Alarms and Events shown when you recall a saved view may vary from the alerts shown in the view when you first saved it, depending on the current state of your network devices.

To filter your view to the alerts you want:

- Click the ≡ as needed to toggle on the floating filter fields at the top of the **Device Alarms** or **Device Events** list. Then, in one or more of the fields, enter or select the criteria that the alerts must match to appear in the list.
- Click the ⚙ to choose the columns shown in the **Device Alarms** or **Device Events** list.
- On the **Device Alarms** window only: Move the **Active Alarms Only** slider to the left to enable display of all alarms, or to the right to display only active alarms.

To save the current view as a new saved view:

1. Filter the alerts on your current view as needed.
2. If a saved view is already displayed, click the ✕ icon next to the saved view's name in the **Saved Views** field. If you don't do this, you will overwrite the current saved view with the current view, and will not be prompted to change the saved view's name.
3. Click **Save View**.
4. Enter a unique name for the new saved view.
5. Click **Save**.

To display a saved view:

1. Next to the **Saved Views** field, click the ⋯. Crosswork displays the **Manage Saved Views** window.
2. Find the saved view you want to display by clicking on the **My Views** or **All Views** tab, selecting an option from the **Sort By** menu, or by entering criteria in the search field with the 🔍.
3. Click on the name of the saved view you want to display. Crosswork changes the alerts list to display the saved view.

To overwrite the current saved view:

1. Display the save view you want to overwrite.
2. Filter the alerts as needed.
3. Click **Save View**. Crosswork overwrites the saved view with the current view.

To delete a saved view:

1. Next to the **Saved Views** field, click the ⋯. Crosswork displays the **Manage Saved Views** window.

2. Find the saved view you want to delete by clicking on the **My Views** or **All Views** tab, selecting an option from the **Sort By** menu, or by entering criteria in the search field with the 🔍.

3. Click the 🗑 next to the name of the saved view you want to delete. Crosswork deletes the saved view.

Export Alerts

Follow these steps to export device alerts for offline storage and analysis.

You must be viewing alarms to export alarms, or events if you want to export events. You can choose to export alerts to comma-separated values (CSV) or PDF file formats.

By default, Crosswork exports all the alerts currently visible in the **Device Alarms** or **Device Events** list. You can limit the contents of the exported file to just the alerts you want by filtering the list, or selecting the checkbox next to the alerts you want, before clicking the 📤.

Step 1 From the main menu, choose **Device Alerts** > **Device Alarms** . Crosswork displays the **Device Alarms** window.

If you want to export events instead of alarms: In the **Show** dropdown, select **Events**.

Step 2 (Optional) Filter the list of events to be exported by filtering columns, or by adding or removing columns using the ⚙ and then filtering again. Use the **More Options** dropdown to choose whether you want to see only current alerts or all alerts, and how often the window syncs the displayed list with the Crosswork database. For alarms only: Move the **Active Alarms Only** slider. You can also check the check box next to the ID of only the alerts you want to export.

For alarms only: Move the **Active Alarms Only** slider. You can also check the check box next to the ID of the alerts you want to export.

Step 3 Click 📤. Crosswork displays an export popup window appropriate for the type of alert you want to export.

Step 4 In the **Name** field, enter the name of the destination file (don't include a filename extension).

Step 5 Using the **Format** button, select **CSV** or **PDF**.

Step 6 Click **OK** to begin the export, and specify the storage location for the new file.

Customize Alerting Devices

Crosswork lets you customize the set of Cisco devices from which you want to receive alerts.

Step 1 From the main menu, choose **Administration** > **System Settings** > **Device Alarm Settings** > **Device Alarm Admin** > **Manager Settings** > **.** Crosswork displays the **Manager Settings** window, with a list of all the Cisco devices from which Crosswork can receive alerts.

Step 2 (Optional) Filter the list of devices by filtering on the **Name** and **Status** column filter fields. You can toggle the filter fields on and off by clicking on the ≡.

Step 3 To start receiving alerts from a device type, click the checkbox shown next to the device type's name and then click **Enable**.

Step 4 To stop receiving alerts from a device type, click the selection checkbox shown next to the device type's name and then click **Disable**.

Step 5 When you are finished making changes, click **Save** to apply them.

Customize Alarm Auto Clear

Crosswork lets you customize whether an alarm can be automatically cleared and how many minutes to wait before automatically clearing it.

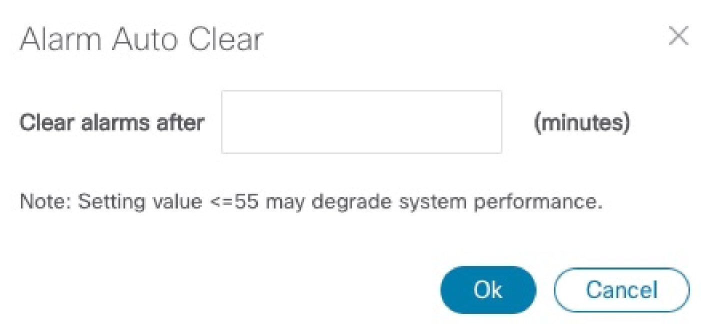
Step 1 From the main menu, choose **Administration** > **System Settings** > **Device Alarm Settings** > **Severity and Auto Clear** Crosswork displays the **Severity and Auto Clear** window, showing the list of all the standard alarm types.

Step 2 (Optional) Filter the list of alarms by entering or selecting values in one or more of the **Name**, **Category**, **Severity**, and **Auto Clear Duration** column filter fields. You can toggle the filter fields on and off by clicking on the ☰.

Step 3 To assign a time after which an alarm will be automatically cleared, click on the check box shown next to that alarm's name in the list. Then click **Alarm Auto Clear**.

Step 4 With the **Alarm Auto Clear** window displayed, enter the number of minutes to wait before clearing in the **Clear alarms after** field. Then click **OK**.

Figure 8: Alarm Auto Clear Window



Note: Setting value <=55 may degrade system performance.

Step 5 To stop an alarm from being automatically cleared, first select it in the list and then click **Revert Alarm Auto Clear**.

Step 6 When you are finished making changes, click **Save** to apply them.

Customize Instructive Text for Alarms

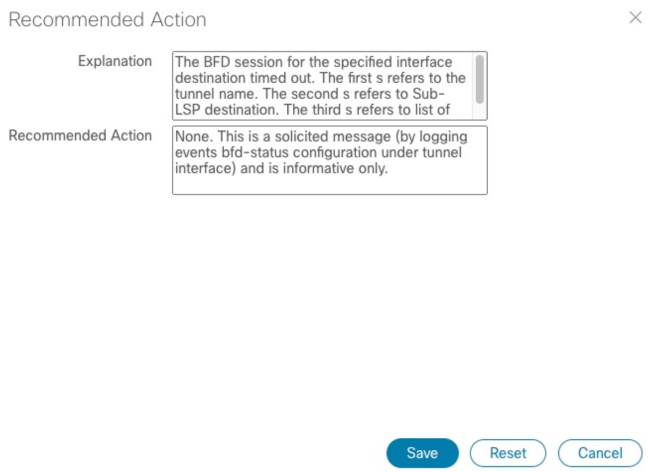
Crosswork enables you customize the instructive "explanation" and "recommended action" text available for each of the alarms in the Crosswork database. If you or another user have made changes to these texts, you can also choose to restore the original text.

Step 1 From the main menu, choose **Administration** > **System Settings** > **Device Alarm Settings** > **Severity and Auto Clear** Crosswork displays the **Severity and Auto Clear** window, showing the list of all the standard alarm types.

Step 2 (Optional) Filter the list of alarms by entering or selecting values in one or more of the **Name**, **Category**, **Severity**, and **Auto Clear Duration** column filter fields. You can toggle the filter fields on and off by clicking on the ≡.

Step 3 To customize an alarm's instructive text, click on the check box shown next to that alarm's name in the list. Then click **Recommended Action** to display the **Recommended Action** window.

Figure 9: Recommended Action Window



Recommended Action

Explanation: The BFD session for the specified interface destination timed out. The first s refers to the tunnel name. The second s refers to Sub-LSP destination. The third s refers to list of

Recommended Action: None. This is a solicited message (by logging events bfd-status configuration under tunnel interface) and is informative only.

Step 4 Click in the **Explanation** and **Recommended Action** fields and enter the text you want. You can enter any form of plain ASCII text in these fields, or edit the text already there. When you are finished, click **Save**.

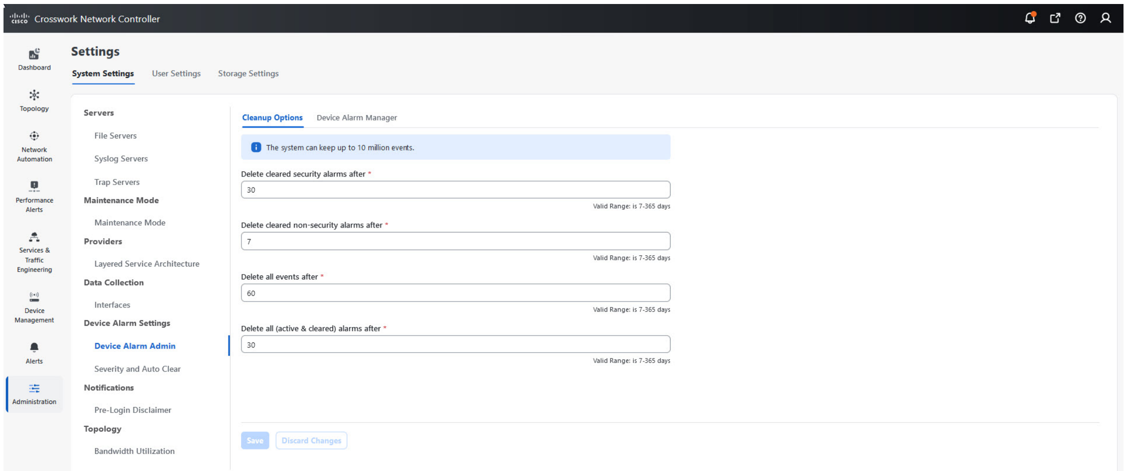
Step 5 To revert back to the original Crosswork instructive text for an alarm: First select the alarm in the list, click **Recommended Action**, and then click **Reset**. When you are finished, click **Save**.

Customize Alert Cleanup

Crosswork can store up to a maximum of 10 million events. Before reaching that limit, the system automatically begins deleting events and active or cleared alarms on a regular schedule. You can view and customize the schedule by following the steps below.

Step 1 From the main menu, choose **Administration** > **System Settings** > **Device Alarm Settings** > **Device Alarm Admin** > **Cleanup Options**. Crosswork displays the **Cleanup Options** window.

Figure 10: Alert Cleanup Options



The system can keep up to 10 million events.

Delete cleared security alarms after *
30
Valid Range: is 7-365 days

Delete cleared non-security alarms after *
7
Valid Range: is 7-365 days

Delete all events after *
60
Valid Range: is 7-365 days

Delete all (active & cleared) alarms after *
30
Valid Range: is 7-365 days

Step 2 Change the cleanup schedule for each type of alert, as needed. To change the schedule, enter the number of days after which Crosswork deletes each type of alert. The valid range is between 1 and 365 days. Entries are required in all fields.

Step 3 When you are finished, click **Save** to apply your changes.

Customize Alarm Severity

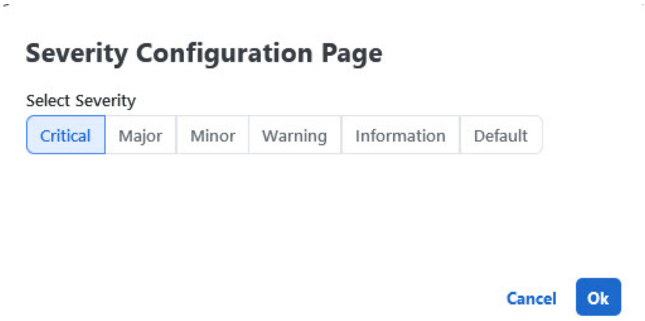
You can customize the Crosswork alarm database to assign your choice of severity levels to particular alarms.

Step 1 From the main menu, choose **Administration** > **System Settings** > **Device Alarm Settings** > **Severity and Auto Clear** Crosswork displays the **Severity and AutoClear** window, showing the list of all the standard alarm types.

Step 2 (Optional) Filter the list of alarms by entering or selecting values in one or more of the **Name**, **Category**, **Severity**, and **Auto Clear Duration** column filter fields. You can toggle the filter fields on and off by clicking on the ≡.

Step 3 To customize the severity of an alarm, click on the check box shown next to that alarm's name in the list. Then click **Severity Configuration** to display **Severity Configuration Page**.

Figure 11: Severity Configuration Page



Severity Configuration Page

Select Severity

Step 4 click on the severity level you want to assign to the alarm. Then click **OK**.

Step 5 When you are finished making changes, click **Save** to apply them.