



Industrial Network Director User Guide

First Published: 2016-09-20

Last Modified: 2022-05-09

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS

CHAPTER 1	Using Industrial Network Director Online Help	1
	Logging in to Cisco IND Application	1
	Before You Begin	1
	Accessing IND Online Help	3

CHAPTER 2	Design	5
	Plug and Play	5
	Inventory	6
	Unclaimed Devices	9
	Profiles	10
	Config Templates	15
	DHCP Helper	16

CHAPTER 3	Operate	19
	Alarms	19
	Alarm Details	21
	Audit Trails	22
	Dashboard	23
	Discovery	24
	Discovery Profiles	26
	Device Access Profiles	27
	Manually Add Device	32
	Single Device Add	33
	Multiple Device Add	34
	NAT Lookup Table	34
	Device Replacement	35

- Expected Behavior for Device Replacement 36
- Device Replacement Prerequisites 37
- Guidelines and Limitations 37
- Inventory 38
 - Licensed Devices 40
 - All Devices 46
 - Device Details 48
 - Licensed Device Details - Switch 48
 - Licensed Device Details - CIP Device 69
 - Licensed Device Details - PROFINET PLC 73
 - Other Device Details 74
 - Port Details 75
 - Device Prerequisite Configuration 76
 - Bootstrap Configuration 78
- Topology 80
 - VLAN Layer 83
 - DLR Layer 83
 - PTP Layer 84
 - REP Layer 85
 - PRP Layer 85
 - MRP Layer 86

CHAPTER 4

Maintain 89

- Cisco Active Advisor 89
- Configuration Archives 90
 - Restore Configuration 92
- Software Images 93

CHAPTER 5

Settings 95

- Alarm Settings 95
- Backup 100
- Certificate Management 101
- Device Pack 103
- Group Management 103

Licenses	105
Classic Licensing	106
Smart Licensing	107
Policy Servers	108
pxGrid	109
System Settings	112
Tags	115
Users	116
User Accounts	116
User Roles	117
Active Sessions	120
Password Policies	120
External Authentication	122

CHAPTER 6

User Interface	123
Buttons and Controls	123
Tasks	125
User Profile Settings	126

CHAPTER 7

Troubleshooting	129
Installer Failures	129
Discovery Failures	129
Device Discovery	129
Topology Discovery	130
Administrative State Change Failures	131
CIP Backplane	131
Page Not Found	132
No Permission	132
Configuration Archive Failures	132



CHAPTER 1

Using Industrial Network Director Online Help

- [Logging in to Cisco IND Application, on page 1](#)
- [Accessing IND Online Help, on page 3](#)

Logging in to Cisco IND Application

IND is a server application and it can be accessed by any client machine that has connectivity to the system on which IND is installed.

Chrome and Firefox are supported browsers.

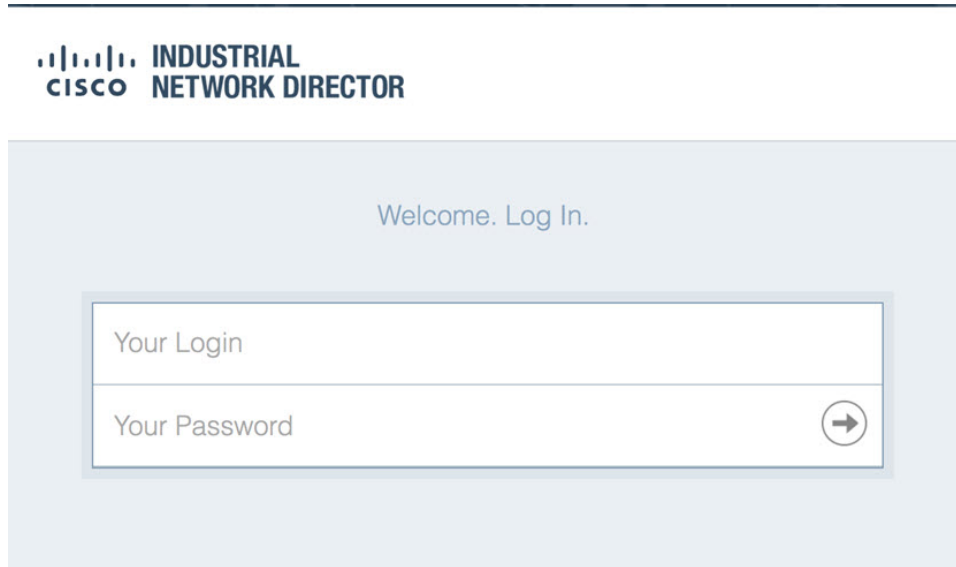
Before You Begin

After an initial install or upgrade, a Setup complete screen displays a check box to launch Cisco Industrial Network Director. Click **Finish** to launch the IND Login URL using the default browser of the system on which IND is installed.

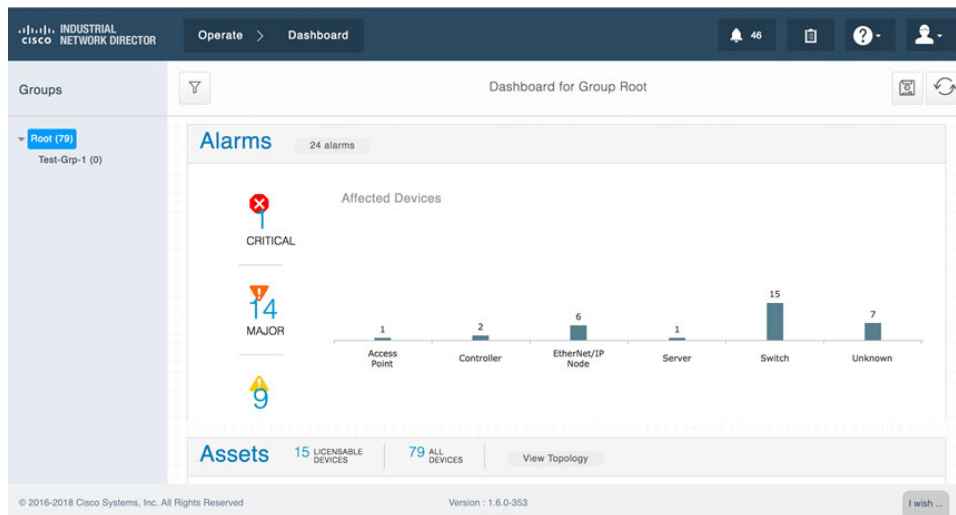
Procedure

- Step 1** On the client machine, open your browser window.
- Step 2** Enter the URL <https://a.b.c.d:portNum> provided at the end of the IND install, where <a.b.c.d> is the IP address of the system where IND was installed. By default, portNum is 8443. If the 8443 value is not available during install, you can enter any available port number.
- Step 3** At the login window that appears, enter the initial Login and Password values provided at completion of the application install.

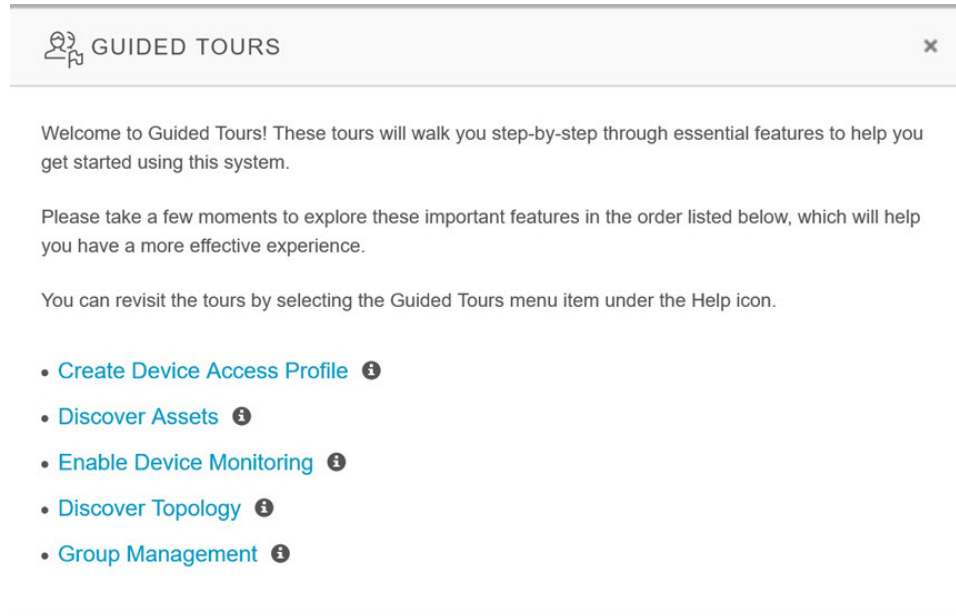
Figure 1: IND Log-in page



- Step 4** Click the arrow in the Your Password field. A window appears requesting you to define a new password.
- Step 5** After you define a new password, the application automatically logs you out. You must reenter your login and password to reenter the application.
- Step 6** When IND opens, the Operate > Dashboard for the Groups Root page appears. There are four summary areas within that page: Alarms, Assets, Traffic Utilization, and Port Counts.



- Step 7** To set up the system:
- Click on the question mark (?) icon in the top right-hand corner of the screen to display menu options: Dashboard Help, Guided Tours, Download Logs, and API Tool.
 - Click on the Guided Tours option to access step-by-step instructions for the system.

Figure 2: Guided Tours

Accessing IND Online Help

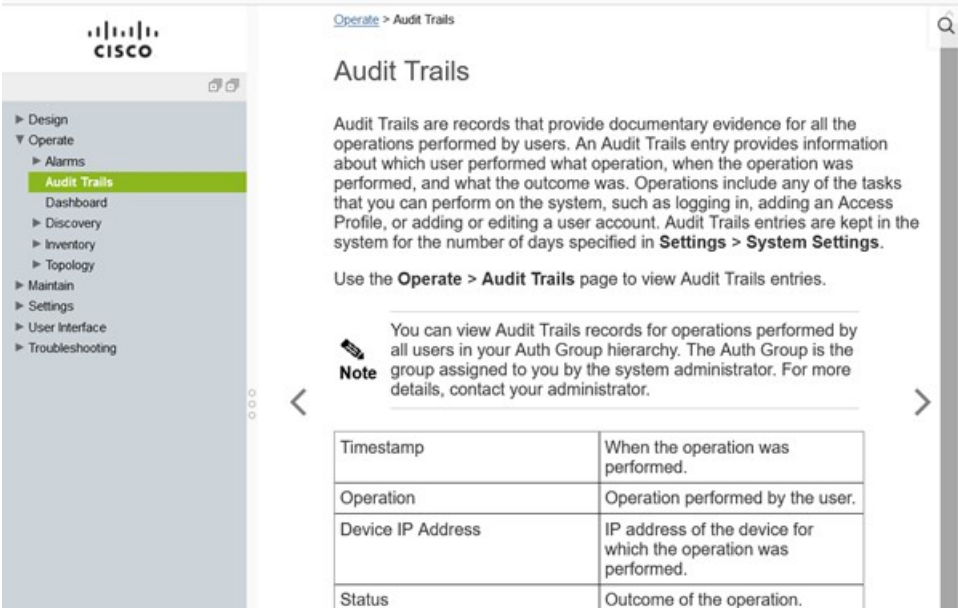
Industrial Network Director has online documentation that you can access from the IND application itself.

To access the online help, after you log in to IND, click on the ? icon in the top right of the IND window. IND displays the related online help topic for the IND page in a new window of your browser. For example, if you are on the Dashboard page, IND displays online help for the Dashboard page. If you are on the Audit Trails page, IND displays online help for Audit Trails, and so on.

Figure 3: Help Icon in IND Window

You can use the navigation menu in the left pane of the online help window to navigate to other topics in the online help.

Figure 4: Online Help Window





CHAPTER 2

Design

- [Plug and Play, on page 5](#)

Plug and Play

Plug-n-Play (PnP) allows you to reduce the costs associated with deployment of network devices by increasing the speed and reducing the complexity of deployments, without compromising security. Using the PnP solution, you can perform Zero Touch installations of equipment in various deployment scenarios and deployment locations.

The system functions as PnP Server to help deploy system-supported network devices with an initial configuration. You configure the system with the information about what configuration file to deliver to the network device to deploy it fully and make it operational. The PnP agent on the device communicates with the PnP server on the system using the open PnP protocol.

PnP Workflow

The PnP workflow for deployment of a new device in the system is listed below. As prerequisites, a template file containing the initial boot configuration information for the device must be pre-configured, and the new device must be connected to the network and powered on.

If the PnP devices in the system have software images with release 15.2.4x, then TLS 1.0 and 1.1 must be enabled for successful communication. If you have such devices, go to **Settings > System Settings > Security Settings** and change the TLS settings to **Weak**. (See [System Settings, on page 112](#).)

1. The network administrator (user in the system with Network Administrator role and Device Management permission) uploads the template file. (See [Config Templates, on page 15](#).)
2. The network administrator creates a PnP Profile with the following information:
 - The template uploaded in step 1.
 - Option to push the configuration to the startup or running configuration.
 - Optional Group.
 - Optional exec commands that require a reboot of the device.
 - Optional Software Image(s) to upgrade devices.
 - PnP match criteria, consisting of the device serial number.

(See [Profiles](#), on page 10.)

3. The new device boots up and the PnP agent on the device is triggered because there is no startup configuration in the NVRAM (new devices do not have any startup configuration by default). As part of the boot process, the PnP agent discovers the PnP server's IP address.
4. After the PnP agent discovers the PnP server, the PnP agent initiates communication with the PnP server. If a PnP request from the agent matches a device serial number, the PnP device status is Certificate-Install-In-Progress.
 - The PnP server obtains the template file to be pushed based on the matching PnP Profile and generates a new configuration file. If the software image corresponding to the device family is selected, it will be pushed to the device. The new configuration file location is pushed, and the PnP status is updated to "Config Success" if the startup configuration is pushed to the device. If the running configuration is pushed to the device, the PnP status is updated to "Discovery Success".



Note The user credentials to access the device must be included in the template file.

- If the option to push the configuration to the running configuration was selected, after config push is successful, discovery of the device is initiated using the Device Access Profile credential information. After the discovery is successful, the device is added to the specified group.
 - If there is an error in the config push, the system continues to retry until a valid template is uploaded.
5. If a PnP request is received from a device that does not match one of the defined PnP Rules, the system creates an entry in the PnP Device table with PnP Status as "Unclaimed". (See [Unclaimed Devices](#), on page 9.)

Inventory

The Inventory page is the opening page of **Design > Plug and Play**. This page displays a list of devices from which the PnP server has received PnP requests, including information about the device and its PnP status.

Name	The device name from the configuration file.
Serial Number	The device serial number.
Product ID	The product ID (PID) of the device obtained through PnP protocol communication between the device and the system.
IP Address	The device IP address from the configuration file or the temporary IP address assigned through DHCP Helper , on page 16.
Last Contact	Time that the PnP device last communicated with the system.

Status	
--------	--

The PnP device status can be one of the following:

- Pending—When a unclaimed device is claimed manually, the device is in pending state, meaning that the PnP server is waiting for the next communication or work request from the device.
- Certificate-Install-In-Progress—Certificate for secure communication was sent to the device and the PnP server is waiting for the response.
- Certificate Success—Response to the certificate was received from the device.
- Authentication Progress—SUDI certificate validation for a device with authentication enabled in the PnP profile is in progress.
- Authentication Success—Device authentication using SUDI certificate was successful.
- Authentication Failed—Device authentication using SUDI certificate failed.
- Device Info Pending—After Certificate success, the image version is obtained from the device.
- Certificate Failed—Response to the certificate failed.
- Image Install Pending—Install of selected image is pending.
- Image Install Success—Install of selected image is successful.
- Config Progress—Initial boot configuration provisioning of the device is in progress.
- Config Success—Initial boot configuration provisioning of the device is successful.
- Save Config Inprogress—After configuration install is successful, the config will be saved to start-up config if the running configuration is pushed to the device.
- BackOffSuccess—After the configuration is pushed successfully to the device, the device sends the Backoff success to IND .
- Discovery in Progress—IND is in the process of discovering the device.
- Discovery Success—IND successfully discovered the device.
- Discovery Failed—The device already exists in

	<p>the IND inventory or no SNMP community string is configured in the device.</p> <ul style="list-style-type: none"> • Unclaimed—If the incoming PnP request could not match any rules under the PnP profile, then the status is "Unclaimed". See Unclaimed Devices, on page 9.
Profile	The PnP profile associated with this device.
Config	Click the View link to display the configuration file pushed to this device.
Details	Click the link to display additional information, if any, for the PnP device status.

Unclaimed Devices

The Unclaimed Devices page lists devices that the system cannot find a match for in the associated PnP profile. You can "claim" the device by using an existing PnP profile and modifying it or by creating a new PnP profile.




Note You can claim only unclaimed devices, and you must claim the device by using only the manual input method and the serial number.

The drop-down menu includes only profiles created using the manual input method.

To claim a device:



1. Select the device(s) in the Unclaimed PnP Devices table, or click  to display devices in a card view that shows an image of the device front panel, along with the PnP inventory details.
2. Click **With Selected**.
3. In the With Selected Unclaimed PnP Devices pop-up window:
 - Click **Delete** to delete the device.
 - Select an existing PnP profile from the drop-down menu to clone from or click **Create a New Profile**, and follow the steps to create the profile described in [Profiles, on page 10](#). When cloning an existing profile, you cannot change the template, Device Access Profile, associated software image, match criteria, or input method.

Click the **Locate** button for a device in table or card view to activate the Locate Switch feature (described in table below).

Name	The device name obtained through PnP protocol communication between the device and the system.
------	--

Serial	The device serial number obtained through PnP protocol communication between the device and the system.
Product ID	The product ID (PID) of the device obtained through PnP protocol communication between the device and the system.
IP Address	The device IP address obtained through PnP protocol communication between the device and the system.
Last Contact	Time that the PnP device last communicated with the system.
Status	The PnP status of the device: Unclaimed.
Locate	Click the icon to send a locate switch command to the device. This feature is used to locate a new switch that is installed in the network. This command makes all system LEDs on the switch blink alternately green and red (LEDs that are in one color blink) for 60 seconds to provide a visual indication of the switch's location.

Profiles

The PnP server uses a profile that you create on the **Design > Plug and Play Profiles** page to determine the configuration file to push to a device. Click the **Profiles** menu tile on the left of the Plug and Play page to display the Profiles page.

There are four basic steps to create a PnP profile, shown at the top of the New PnP Profile or Edit PnP Profile page:

1. **Attributes**—Includes profile name, template, whether to enable Device Authentication, whether to push to startup or running configuration, Device Access Profile, Group, pre-configuration commands, exec commands, and software image(s).
2. **Devices**—Includes the device Serial Number as match criteria, which you can enter manually or upload as a Comma-Separated Values (CSV) file. The CSV file includes values for the template variables. If you use a CSV file, the profile creation process skips step 3.



Note You can create a PnP profile without entering any serial numbers, and edit the profile later to specify devices.

3. **Template Values**—If you manually entered match criteria in Step 2 above, enter the values that the system will substitute for the template values in this step.
4. **Preview**—Displays the configuration file that the system will push to the device.

- Click **Create** to create a new profile. Click **Next** to go to the next step in the process, click **Back** to return to the previous page, and click **Save** to save the profile.

- Click **Upload** to upload an existing PnP profile, and then click **Browse** to select a file.
- To edit an existing profile, click the link in the Profile column in the Profiles table.



Note You cannot change the input method (manual or CSV) or Match Criteria (Serial Number) of an existing profile.

- To delete a profile, select it from the list in the table, click **With Selected**, and then click **Delete** in the With Selected Profiles pop-up window.

Table 1: Profiles Table

Profile	Name of the profile. Click the link to edit the profile.
Last Updated	Timestamp for when this profile was created or modified.
Template	Name of the template that this Profile uses. Click the link to view the configuration file that the system will push to the selected device. The template variables are replaced with the values that you specified (in Template Values or in the CSV file) and are displayed in red text. If there is no device associated with the profile, the Config Template will just show the content of the template without variable substitution.
Devices	The number of PnP devices that use this profile.
Download	Click the down arrow to download a zip file of the profile in JSON format and a version file containing the system version.

Attributes

Name	Name of the profile. Profile name can be from 1 - 50 characters long and can contain the following characters: A-Z, a-z, 0-9, underscore (_), dash (-), spaces, and all non-ASCII characters. The name cannot start or end with underscore (_), dash (-), or spaces.
Configuration Template	Select an available template for this profile from the drop-down menu or click the link to upload a template. (See Config Templates, on page 15.)

Device Authentication	<p>Select Enable to specify that device authentication should be performed on the PnP server using a Secure Unique Device Identifier (SUDI) certificate (a X.509 compliant certificate). This option ensures that the PnP server communicates only with a device that is validated through the SUDI certificate.</p> <p>Select Disable to not perform device authentication.</p> <p>Note When Device Authentication is enabled, the PnP workflow will fail with "Authentication Failed" if the device is running an IOS image that does not support the PnP device auth service.</p>
Apply Configuration Template to	<p>Click the green toggle button to select whether to apply the Configuration Template to the startup configuration or running configuration of the device. The default is startup configuration.</p> <ul style="list-style-type: none"> Choose Startup Configuration if the IP address assigned to the device in the Configuration Template is in a subnet where the device cannot communicate with IND after PnP commissioning. <p>With this option, you will need to configure IND to discover the device.</p> <ul style="list-style-type: none"> Choose Running Configuration if the device can communicate with IND after PnP commissioning using the credentials in the specified Access Profile. <p>With this option, IND can discover the device and it will automatically appear in the system inventory.</p> <p>Note If applying the Configuration Template to the running configuration, make sure that the network connection between IND and the switch remains active and is not affected by any configuration that is present in Config Template.</p>
Device Access Profile	<p>If you choose to apply the Configuration Template to the Running Configuration, select the Device Access Profile that allows IND to discover the device after PnP commissioning. See Device Access Profiles, on page 27 for information about creating a Device Access Profile.</p>

Assign to Group	<p>If you choose to apply the Configuration Template to the Running Configuration, select the Group to which the device will be assigned after discovery.</p> <p>Note The Context Group drop-down menu lists the groups and subgroups that you can access based on your Auth Group. The Auth Group is the group assigned to you by the system administrator. For more details, contact your administrator.</p>
Pre-configure device before commissioning?	<p>Check the check box to select whether to apply a set of configuration CLI commands to the device running configuration, and enter the commands in the text box. These commands are executed before the configuration file is applied to the device.</p> <p>Use this option for device configuration commands that require a reboot to take effect, such as setting the SDM template.</p> <p>The default is No (do not pre-configure the device).</p> <p>Note The system does not parse the commands that you enter, so ensure the validity of commands before deployment.</p>
Execute commands on device before commissioning?	<p>Check the check box to select whether to apply a set of EXEC CLI commands to the device running configuration, and enter the commands in the text box. These commands are executed before the configuration file is applied to the device.</p> <p>Use this option for device configuration commands that require a reboot to take effect, such as activating a right-to-use license on a device.</p> <p>The default is No (do not execute commands on device).</p> <p>Note The system does not parse the commands that you enter, so ensure the validity of commands before deployment.</p>
Upgrade device software	<p>Check the check box to select up to three software images (one per device type) from the drop-down menu to associate with the PnP profile, or click the link to upload a new software image.</p> <p>You can also upload and manage software images from the Software Images page. (See Software Images, on page 93.)</p> <p>PnP sends the image specified in the profile to devices based on the device type.</p>

Devices

Match Criteria	Serial Number Select Serial Number from the drop-down menu to match a PnP request from a device to a PnP profile.
Input Method	Click the green toggle button to select whether to enter device serial numbers manually or upload a list of devices in CSV file format.
Device List	For manual input, enter the list of device serial numbers, separated by commas. For CSV input, click Browse to select a file.

Template Values

If you selected to use the manual method of entering device information, enter the values that will be substituted for the template variables.

Template Content	Displays the content of the template that you uploaded in step 1, Attributes, with variables shown in red text.
Value	For regular input, enter an alphanumeric string for the replacement value.
Base Value	For range input (see Range below), enter an alphanumeric string. The replacement value is Base Value concatenated with Index (see Index below).
Starting Index	Enter a number for the starting number of the device list. The replacement value is Base Value concatenated with Index. For example, if the Base Value is "Cell-2 SW" and the starting index is 5, the value for the first device in the device list is "Cell-2 SW5", the value for the 2nd device is "Cell-2 SW6", and so on.
Range	Click the green toggle button to select whether to enter a single value or a range of values.

Preview

Name	Name of the profile entered in Attributes.
Group, Device Access Profile, pre-config commands, exec commands, software images	Attributes that you selected for this profile.

Device List	The devices that you have specified (either by manual or CSV input) for this profile. Select a device from the drop-down list to display the configuration template for that device.
Config Template	The configuration file that the system will push to the selected device. The template variables are replaced with the values that you specified (in Template Values or in the CSV file) and are displayed in red text. If there is no device associated with the profile, the Config Template shows the content of the template without variable substitution. Click Save to save the profile or click Back to make changes.

Config Templates

A config template is a configuration file that you create and upload to the system. As described in [Plug and Play, on page 5](#), you associate the template with a PnP profile that the system uses to generate a configuration file to push to the specified device. The template contains variables (for example, `${hostname}`) that the system substitutes with device-specific values that you specify when you create the PnP profile. A sample config template is shown below.



Note You can use a simple text editor to create the configuration template file and save it with a .ftl extension. No conversion tool is required.

To upload a template file, click **Upload**. In the Upload a Template popup, click **Browse** to select a file. Template file names must have an ".ftl" extension.

After you upload a template, it is listed in the Templates table. Click the link in the Template Name column to display the template content.

Template Name	Name of the template.
Size (Bytes)	Size of the template in bytes.
Uploaded Time	Date and time when template was uploaded to the system.
Profiles	Number of PnP profiles that use this template. Click the link to display the list of profiles.

Sample IOS Config Template

```
hostname ${name}
!
username ${localPriviledgedUser} privilege 15 password 0 ${localPriviledgedPassword}
!
```

```

vlan ${mgmt_vlan}
name vlan.Management
vlan ${data_vlan}
name vlan.DataTraffic
!
Interface ${interface_id}
 ip address ${ipaddress} ${subnetmask}
 no shutdown
!
ip default-gateway ${ipDefaultGateway}
!
end

```

Sample IE 1000 Config Template

```

hostname ${hostname}
enable password ${enablePassword}
username ${username} privilege 15 password unencrypted ${password}
!
vlan {mgmtVlan}
!
!
!
!
ip route 0.0.0.0 0.0.0.0 ${ipDefaultGateway}
no ip name-server 0
no ip name-server 1
no ip name-server 2
no ip name-server 3
snmp-server
snmp-server community ${snmpPassword} ip-range 0.0.0.0 0.0.0.0 ${snmpPassword}
aaa authentication login telnet local

interface ${interfaceName}
 ip address ${interfaceIpAddress} ${interfaceSubnetMask}
!
line console 0
!
line vty 0
!
line vty 1
!
line vty 2
!
line vty 3
!
line vty 4
!
line vty 5
!
line vty 6
!
line vty 7
!
end

```

DHCP Helper

The first step in the Plug-and-Play workflow is for the network device to discover the Plug-and-Play server. The DHCP Helper is used to assign a temporary DHCP IP address to the device so it can contact this

Plug-and-Play server. This feature should be used only if external DHCP server, DNS, or Cloud Redirect discovery options are not available.

The system includes an integrated DHCP server that has a predefined private IP subnet in which leases are supplied to the requested DHCP clients. Use the DHCP Helper page to enable the DHCP service and allow the system to assign dynamic IP addresses for PnP devices, with the following restrictions:

- The DHCP service operates in a single predefined private subnet: 192.168.200.0/24
- The pool size is 245 (a total 245 IP addresses are available to be assigned)

DHCP Helper provides a 30 minute lease only. However, a device can renew the lease as long as the device is reaching the system and needs the IP address. Generally, the device should keep the IP address until PnP provisioning is complete.

If the device is not able to reach the system, the lease will be released after the duration time expires. The system may reassign that IP address to another device.



Note Before you can use DHCP Helper, you must first manually assign IP address 192.168.200.1 and netmask 255.255.255.0 to the network interface used for Plug-and-Play services.



Note Ensure that Windows network drivers are correctly installed before you enable DHCP Helper. If you do not see leases offered, run Wireshark to verify that DHCP packets are coming into Windows.

To use DHCP Helper, click the green toggle button to enable it. You cannot disable DHCP Helper if there are any active leases.

Pool Size	Size of the DHCP pool: 245
Leased	Number of addresses that have been assigned.
Available	Number of addresses remaining in the pool.
Scope	Subnet from which addresses are assigned.
Interface Name	The interface face on which subnet 192.168.200.0/24 is configured.
Lease Duration	Time before lease expires (30 minutes). A lease holder must send a request to renew the lease before expiry. The lease is extended by the Lease Duration. After expiry, the lease cannot be held by the client.
DHCP Leases	
IP Address	The device IP address assigned from the pool.
Mac Address	The device MAC address.

Expiration	Time when the lease will expire.
Hostname	The device host name.



CHAPTER 3

Operate

- [Alarms, on page 19](#)
- [Audit Trails, on page 22](#)
- [Dashboard, on page 23](#)
- [Discovery, on page 24](#)
- [Inventory, on page 38](#)
- [Topology, on page 80](#)

Alarms

Alarms are event messages that IND receives from discovered devices. The devices that the system monitors for alarm and other information include:

- Licensed devices in the Licensed state, including Cisco Industrial Ethernet (IE) switches, CIP backplane devices, DLR Supervisor devices, MRP devices, PRP devices, and PTP enabled devices.
- Unmanaged and unlicensed Cisco IE devices.

Alarms provide information about the health of the infrastructure that can help you troubleshoot and resolve issues. For alarm descriptions, see [Alarm Settings, on page 95](#).

The system receives SNMP traps for Event notifications from devices and correlates these events with alarms. Alarms and events are stored in the system database for the user-defined retention period (see State in table below).




Note IND does not update the inventory information automatically on receiving traps from licensed devices. Refresh the device by clicking **Retrieve Device Data** in the inventory details page or wait for IND to poll the device according to pre-configured polling intervals to retrieve the latest inventory information from the device.



Note To process traps from unmanaged devices, the device must be already configured with IND as an SNMP Server host to receive traps from the device.

The following alarm features are not supported for unmanaged and unlicensed devices: Device Detail page with the Alarm banner and Events tab, email alerts for alarms, and Link up discovery task trigger when portUp/interfaceUp Trap is received.



The number of new alarms in the system is shown at the top of every page by the icon . The alarm status of individual devices in the system is shown in table and topology views by an alarm severity icon (see table below).



Note To enable or disable an alarm or change the default severity of an alarm, go to the **Settings > Alarm Settings** page.

You can manage alarms by viewing alarm details, opening or closing an alarm, assigning it to someone, and adding notes on the Alarm Details page.

- Use Alarm Filters in the left pane to display alarms by Source (Device or System), Groups, Assigned To, Category, Severity, State, or Type. The number of alarms for the filter(s) you select is shown next






to the filter button

- Click the link under Last Update to go to the [Alarm Details, on page 21](#) page for the alarm.
- To reopen or close an alarm, select it from the list, click **With Selected**, then select **Reopen** or **Close** from the drop-down list in the With Selected Alarms pop-up window.
- To assign an alarm to a user, select the alarm from the list, click **With Selected**, then select a user from the drop-down list in the With Selected Alarms pop-up window.



Note You can also reopen, close or assign an alarm on the Alarm Details page.

Severity	<p>Alarm severity:</p> <ul style="list-style-type: none"> •  Critical •  Major •  Minor <p>You can change the default severity on the Settings > Alarm Settings page.</p>
----------	--

Last Update	<p>Timestamp of last Set/Clear Event.</p> <p>Click the link to go to the Alarm Details page for the alarm.</p>
State	<p>The state of the alarm:</p> <ul style="list-style-type: none"> • New—Beginning state; alarm appears on Alarms page and can be closed or assigned. • Assigned—Alarm is assigned to a user with Alarm Management permission. User can add notes to alarm. • Closed—Alarm is manually closed by the user or auto-closed by the system upon receiving clear event. Closed alarm can be assigned and user can add notes to alarm. <p>Closed alarms are pruned from the system based on the retention period that you specify in Settings > System Settings. New and assigned alarms are not pruned.</p>
Device	The device that generated the alarm.
Type	Description of the alarm.
Message	Alarm message.
Assigned To	<p>User with Alarm Management permission who owns this alarm.</p> <ul style="list-style-type: none"> • The owner of an alarm can be changed to a different user by any user with alarm management permission. • Once the ownership of an alarm is set, it cannot be removed (that is, set back to no owner).
Category	<p>Alarm category.</p> <p>Alarm categories are listed on the Settings > Alarm Settings page.</p>
Affected Devices Count	The number of devices impacted by this alarm.

Alarm Details

The Alarm Details page appears when you click the Last Update link on the Alarms page or click **View Details** in the alarm banner at the top of the Licensed Device Details page for a switch. The color of the alarm banner corresponds to the alarm severity: red (critical), orange (major), yellow (minor). The banner for a closed alarm is gray. Alarm Details shows the source module (for example, port number) for the alarm, which allows you

to obtain information about the alarm at the device level. You can also add notes and view events and history for the alarm.



Note You can view only the alarm records for the devices in your Auth Group hierarchy. The Auth Group is the group assigned to you by the system administrator. For more details, contact your administrator.

- To assign an alarm to a user, select a user from the drop-down list in the alarm banner.
- To reopen or close an alarm, click **Reopen Alarm** or **Close Alarm** in the alarm banner.
- Click the links under This Device to go to [Device Details, on page 48](#) or [Port Details, on page 75](#).
- Click the links under Affected Devices to go to [Device Details, on page 48](#) or [Port Details, on page 75](#) of connected devices impacted by this alarm.



Note Links are shown only for the devices in your Auth Group and subgroups. For other devices, the links are disabled.

- Click **New Note** on the Alarm Notes tab to add a note to the alarm. The note cannot contain "<" or ">" and cannot be longer than 255 characters. Type your note in the text box and click **Add**.
- Click the **Alarm Events** tab to view the events associated with the alarm.
- Click the **Alarm History** tab to view the details about the alarm history, including owner and state changes.

Audit Trails

Audit Trails are records that provide documentary evidence for all the operations performed by users. An Audit Trails entry provides information about which user performed what operation, when the operation was performed, and what the outcome was. Operations include any of the tasks that you can perform on the system, such as logging in, adding an Access Profile, or adding or editing a user account. Audit Trails entries are kept in the system for the number of days specified in **Settings > System Settings**.

Use the **Operate > Audit Trails** page to view Audit Trails entries.



Note You can view Audit Trails records for operations performed by all users in your Auth Group hierarchy. The Auth Group is the group assigned to you by the system administrator. For more details, contact your administrator.

Timestamp	When the operation was performed.
Operation	Operation performed by the user.
Device IP Address	IP address of the device for which the operation was performed.

Status	Outcome of the operation.
Username	User who performed the operation.
Remote User	Indicates if the user who performed the operation is a local user or a remote user.
User IP Address	Client IP address.
Details	Details about the operation. Click the link to display details in a pop-up window.

Dashboard

The Dashboard provides a snapshot view of assets (Licensed Devices and All Devices) by group. You can drill down in the group hierarchy to monitor a group of interest. When you first log in, by default, the system displays the Dashboard for the top level group in the hierarchy. (For information about groups, see [Group Management, on page 103.](#))



Note The Dashboard displays devices based on the Context Group drop-down menu selection. The Context Group drop-down menu lists the groups and subgroups that you can access based on your group assignment. See [Buttons and Controls, on page 123](#) for information about the Context Group menu.

- Click a group name in the left pane to display the dashboard for a different group.

The dashboard is organized into the following areas: Alarms, Assets, Traffic Utilization, and Port Counts.

Alarms

The left side of the Alarms area of the dashboard shows the number of alarms for devices in the group by severity (critical, major, and minor). The bar chart shows the number of affected devices by type.

- Click the link at the top of the Alarms area to view the list of alarms for the group on the **Operate > Alarms** page.

Assets

The Assets area shows the total number of devices by type. The number of Licensed Devices and their state (Licensed or Unlicensed) is shown as a pie chart. The number of All Devices is shown by type in a bar chart.

- Click **View Topology** to go to the Topology page for the group and subgroups.

Traffic Utilization

Traffic Utilization shows a list of the top five Licensed network devices and network ports by traffic utilization. The top five Licensed devices are selected based on Average Utilization, and the top five network ports are selected based on Rx Utilization.

- Click the link in the Device column to go to the Device Details page for the device.

- Click the link in the Port column to go to the Device Details or Port Details page for the device or port.
- Click the link in the Connected Device column to go to the Device Details page for the connected device.



Note Links are shown only for the devices in your Auth Group and subgroups. For other devices, the links are disabled.

Port Counts

Port Counts shows a summary of the port utilization for the group. For each port type (copper, SFP fiber, and dual-purpose), the data includes the total number of ports, number of unused ports, and number of ports in operation and their speed.

- Hover the mouse over a section of the chart to show the number of ports in the displayed category (Unused, 10Mb/s, 100Mb/s, or 1000Mb/s).

Discovery

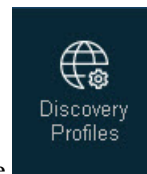
Devices that connect to the Industrial Ethernet (IE) switch network represent the *assets* that the system can discover on the network.

The system supports two types of discovery:

- **IP Scan:** Uses one or more IP addresses in a range as search criteria to locate the devices within that range.
- **Link Layer:** Starts with one IP address and discovers the network hop-by-hop until the Hopcount Limit is reached.

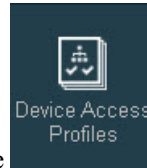
Use the **Operate > Discovery** page to configure a Discovery Profile that defines the parameters for the asset discovery and to run a scan of the network. You can also configure a Device Access Profile that defines the protocols to use for discovery and the credentials that IND uses to access a device.

- Click **New Discovery Profile** on the upper left of the page to create [Discovery Profiles](#).

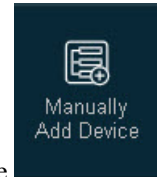


Click the **Discovery Profiles** menu tile on the left of the page to return to the Discovery Profiles page.

- To make a copy of an existing discovery profile, click on the Name of the discovery profile in the table and select **Duplicate Discovery Profile** on the Edit Discovery Profile page. A new discovery profile window appears with the name (existing_discovery_profile_name)_copy. Make any changes needed and save to create the copied discovery profile.
- To delete a profile, select it from the list and click **With Selected**, and then click **Delete** in the With Selected pop-up window.



- Click the **Device Access Profiles** menu tile on the left of the page to configure [Device Access Profiles](#).



- To [Manually Add Device](#) to the IND inventory, click the Manually Add Device menu tile on the left of the page.



- Select the [NAT Lookup Table](#) menu tile to import or export Network Address Translation (NAT) mapping information.
- To view discovered assets go to **Operate > Inventory**.

Name	Name of the Discovery Profile. Click the profile name link to edit the Discovery Profile.
Type	Type of discovery: IP Scan or Link Layer.
IP Address	IP address range or starting IP address for the scan.
Device Access Profile	Device Access Profile associated with this Discovery Profile.
Last Run	To view the status and results of the scan, click the timestamp in the Last Run column or go to Operate > Tasks .
Actions	Click Scan Now to run a scan with the selected Discovery Profile.

Discovery Profiles

Table 2: New Discovery Profile

Name	<p>Name of the Discovery Profile.</p> <p>The name can be from 1 - 50 characters long and can contain the following characters: A-Z, a-z, 0-9, underscore (_), dash (-), spaces, and all non-ASCII characters. The name cannot start or end with underscore (_), dash (-), or spaces.</p>
Discovery Mechanism	<p>Select the mechanism that the system will use to discover assets:</p> <ul style="list-style-type: none"> • IP Scan: Uses protocol based on the Device Access Profile and IP address range. Enter the Start IP, End IP, and Netmask. • Link Layer: Uses LLDP/CDP and starting IP address. Enter the Start IP. Optionally, you can specify a Hopcount Limit to stop the link layer discovery after the specified number of hops. The default Hopcount Limit is 5.
Discover Related Devices	<p>Click the toggle button to select whether the system attempts to discover related devices.</p> <p>When the system discovers a device listed in the IP scan range or link layer hop count, it will try to glean additional network related information from the device and discover other devices that have network associations with it.</p> <p>Note In IND, Neighboring devices are discovered with the help of CDP, LLDP, and the MAC address table.</p> <p>When Discover Related Devices is enabled, IND discovers the neighbor devices that were found with the help of CDP/LLDP/MAC using the same device access profile. All the neighboring devices should respond to the protocols selected in the access profile for neighbor discovery to be successful.</p> <p>For neighboring devices found through the MAC address table, MAC address to IP resolution should be successful for the devices to be discovered in IND.</p>

Device Access Profile	<p>Select an existing Device Access Profile from the drop-down list.</p> <p>Click the link Create New Device Access Profile to open the New Device Access Profile page. See Device Access Profiles, on page 27.</p>
Assign to Group	<p>Select a group from the drop-down list.</p> <p>Devices discovered using this profile are assigned to the selected group. If no group is selected, devices are assigned to the default Root group.</p> <p>Create groups on the Settings > Group Management page.</p> <p>Note The Context Group drop-down menu lists the groups and subgroups that you can access based on your Auth Group. The Auth Group is the group assigned to you by the system administrator. For more details, contact your administrator.</p>

Device Access Profiles

Device Access Profiles allow you to create and manage access credentials that can be used by a device or by a Discovery Profile. You can also specify the protocols that IND uses to discover a device. After you create a Device Access Profile, you can select it for a [Discovery Profiles](#). The Device Access Profile is applied to the devices specified in the Discovery Profile that are discovered through a scan of the network. The values specified in the access profile must match the values configured on the set of devices that the system will manage.

The Device Access Profiles page displays a list of Access Profiles with the associated protocols, devices, and Discovery Profiles.

- To create a profile, click **New Device Access Profile**, enter the access credentials, and click **Save**.
- To edit an existing profile, click on the link in the Name column.
- To make a copy of an existing discovery profile, click on the discovery profile and select **Duplicate Discovery Profile**. A new discovery profile window is shown with the name (existing_discovery_profile_name)_copy. Make any changes needed and save to create the copied discovery profile.
- To delete a profile, select it in the list, click **With Selected**, and then click **Delete** in the With Selected Device Access Profile pop-up window.

Table 3: New Device Access Profile

Simple, Advanced	Click the green toggle button to display or hide expanded access settings for different protocols.
------------------	--

Name	Name of the Device Access Profile. The name can be from 1 - 50 characters long and can contain the following characters: A-Z, a-z, 0-9, underscore (_), dash (-), spaces, and all non-ASCII characters. The name cannot start or end with underscore (_), dash (-), or spaces.
Description	(Optional) Description of the Device Access Profile. The description can be from 1-255 characters long.
Protocols	Select one or more of the available protocols to be used for device discovery.
SNMP Settings	
V3, V2C, V1	SNMP version the system uses to discover the device. At least one SNMP version is required. SNMP values must match the ones configured on the device. You can select multiple SNMP versions, with up to 1 SNMPv3 and up to 5 SNMP V1 and V2C credentials in a single Device Access Profile. During asset discovery, when this Device Access Profile is associated with a Discovery Profile, the system loops through all the available credentials until the device is accessed. After the first iteration, the next time the system contacts the device, it uses the last successful credentials in the Device Access Profile. Note SNMP V1 cannot be used to manage Licensed devices. <ul style="list-style-type: none"> • V3—SNMP version 3, user-based security model that adds user names, authentication, and encryption for security. • V2C—SNMP version 2c, community-based security model. • V1—SNMP version 1, community-based security model.
User Name	User name the system uses to manage the discovered device. This user name must be pre-configured on the device.

Mode	<p>(SNMP V3 only)</p> <p>Indicates the security level for this user:</p> <ul style="list-style-type: none"> • Authentication, No Privacy—Authentication but no encryption. • Authentication, Privacy—Authentication and encryption. This is the default. • No Authentication, No Privacy—No authentication or encryption.
Authentication Type	<p>(SNMP V3 only when Mode is Authentication, Privacy or Authentication, No Privacy)</p> <p>The authentication protocol for the user:</p> <ul style="list-style-type: none"> • SHA—Secure Hash Algorithm authentication protocol. • MD5—MD5 Message-Digest Algorithm. <p>Default authentication protocol is SHA.</p>
Authentication Password	<p>(SNMP V3 only when Mode is Authentication, Privacy or Authentication, No Privacy)</p> <p>A string (minimum length of 8 characters) identifying the authentication password phrase.</p>
Privacy Type	<p>(SNMP V3 only when Mode is Authentication, Privacy)</p> <p>The privacy protocol for the user:</p> <ul style="list-style-type: none"> • AES128—128-bit Advanced Encryption Standard. • DES—Data Encryption Standard. <p>Default privacy protocol is AES128.</p>
Privacy Password	<p>(SNMP V3 only when Mode is Authentication, Privacy)</p> <p>A string (minimum length of 8 characters) identifying the privacy password phrase.</p>
Community Strings	<p>(SNMP V1 and V2C only)</p> <p>Community access string for read access to the device using SNMP V1 or SNMP V2C.</p> <p>Enter a list of up to 5 community strings. Display must be in plain text to add community strings.</p> <p>Default read community string is "public".</p>

Timeout	(Advanced settings only) Number of seconds to wait for a response to an SNMP request. Range: 1 - 60 Default: 5
Port #	(Advanced settings only) Specifies the port the SNMP agent will listen on. Range: 1 - 65535 Default: 161
Retries	(Advanced settings only) Number of times to send an SNMP request after a timeout occurs. Range: 0 - 2 Default: 1
Telnet/FTP/HTTP and SSH/SCP/HTTPS	
User Name	User name the system uses to manage the discovered device. This user name must be pre-configured on the device.
Password	The User Mode password for this user name. This password must be pre-configured on the device.
Enable Password	The Enable password for this user name, used for Privileged Mode. This password must be pre-configured on the device.
HTTP Port #	(Telnet/FTP/HTTP, Advanced Settings only) Port number used to access the device over HTTP. Default: 80
Telnet Port #	(Telnet/FTP/HTTP, Advanced Settings only) Port number used to access the device over Telnet. Default: 23
HTTPS Port #	(SSH/SCP/HTTPS, Advanced settings only) Port number used to access the device over HTTPS. Default: 443

SSH Port #	(SSH/SCP/HTTPS, Advanced settings only) Port number used to access the device over SSH. Default: 22
Device Certificate	Select Self-Signed or CA Certificate. For CA Certificate, select the certificate from the drop-down menu.
OPC UA	
Security	The security mode: <ul style="list-style-type: none"> • None • Sign • SignAndEncrypt
Security Policy	<ul style="list-style-type: none"> • When the security mode is none, the security policy is also none. • When the security mode is Sign or Sign and Encrypt, the security policy can be Basic128RSA15, Basic256, or Basic256SHA256. • For Sign and Sign&Encrypt modes, certificate handshake takes place. Select Self Signed or CA Certificate to use for certificate handshake. The Server has an option of automatically accepting client certificates during runtime.
Port	(Advanced settings only) Port used to connect to the OPC UA server.
User Mode	Enter the user name and password for user authentication mode. If user mode is not enabled, it is set to anonymous/guest mode.
Device Certificate	(Only when security mode is Sign or Sign and Encrypt) Select Self-Signed or CA signed Certificate. For CA Certificate, select the certificate from the drop-down menu. If the desired CA certificate is not listed in drop down list, add a new CA certificate by clicking Add a new certificate . Note By default, the system certificate used for OPC-UA is set to self-signed certificate.

PROFINET, BACNet, Modbus	
Timeout, Retries, Port # (BACNet)	Enter values for timeout and retries within the allowed ranges. For BACNet, enter the number of the port used to connect to the BACNet device. The default is 47808.

Manually Add Device

You can manually add endpoint devices to the IND inventory when the devices cannot be discovered OR when the devices do not return required information such as MAC address and IP Address, or the devices cannot respond to the discovery protocol communication supported by IND. Manually adding these devices allows IND to support features such as Tagging, Assigning to Group, and sending asset information to ISE through the pxGrid service for the devices. The following table shows the IND feature support for manually added devices compared to those added through link up or on demand discovery.

Devices	Move to License State	Device Inventory and Metrics	Device Data Refresh	Connected Links Column in Inventory	Topology with Links to Neighbor(s)	Alarms & Events	Assign to Group	Assign Tags	Send Asset Info to ISE via pxGrid
Devices Added by On Demand Link Up Discovery	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Devices Added by Manual Device Addition	No	No	No	No	No	No	Yes	Yes	Yes

Users with Discovery permission are allowed to add devices. You can add a single device or use a CSV file to perform bulk device addition, as described in [Single Device Add, on page 33](#) and [Multiple Device Add, on page 34](#). The devices you can add manually include devices that run the following protocols: CIP, PROFINET, Modbus, BACnet, NetBIOS, OPC UA, SNMP, and unknown protocol devices. Manual device addition is not supported for devices that can be Licensed (including switches and CIP backplane devices), and manually added devices cannot be moved to the Licensed state. You must add a separate device for each module for multi-module CIP devices.



Note The Device Details page for manually added devices includes Added By and Added Time fields that show which user added the device and when it was added. You can also update the information for manually added devices from the Device Details page. The added or modified device information notification is sent to the ISE through the pxGrid service. You cannot change the IP address or protocol for the device. For more information, see [Other Device Details, on page 74](#).

IND does not interact or communicate with manually added devices, so no Access profile is set, and no Topology discovery is performed for the devices. However, if there are discovered devices connected to the manually added devices and you run an on-demand Topology discovery, links between a discovered device connected to a manually added device are shown from the neighbor information retrieved from the discovered devices.

Single Device Add

To manually add a device, go to **Operate > Discovery** and click the **Manually Add Device** menu tile on the left of the Discovery page. Enter the information for the device. The device IP address is mandatory; all other fields are optional.

Name	The device name. If you do not specify a name, the IP address is used by default.
Description	Description of the device.
IP Address	The device IP address.
MAC Address	The device MAC address.
Protocol	The device protocol. Select the protocol from the drop-down list: UNKNOWN, BACnet, CIP, Modbus, NetBIOS, PROFINET, SNMP, or OPC UA.
Device Type	Select the device type from the drop-down menu or enter the device type text manually. Available device types are based on the protocol you select for the device.
Serial Number	Vendor-specific serial number string for the device. It is recommended that you add the Serial Number for CIP Protocol devices.
Vendor	Name of the device manufacturer.
Product ID	Asset tracking identifier of the device.
Hardware Version	Device hardware version number.
Software Version	Software revision string for the device.

Group	Select the Group to assign the device to from the drop-down menu. The default Group assignment is the Root Group.
Security Tag	Select a Security Tag for the device from the drop-down menu.

Multiple Device Add

To manually add several devices at once, go to **Operate > Discovery** and click the **Manually Add Device** menu tile on the left of the Discovery page. On the **Multiple Device Add** tab, click the link for **Devices_Template.csv** to download the template for the Comma Separated Values (CSV) where you can enter the information for the devices. You can manually add up to 500 devices at once.

Enter the information one row for each device. Refer to the field descriptions in [Single Device Add, on page 33](#) for a description of the fields in the CSV template. The device IP address is mandatory; all other fields are optional.



Note Devices are assigned to the Root group if you do not specify a Group ID.

Group and Security Tag columns in the CSV file accept only the ID but not the name. The IDs can be retrieved through the REST APIs. You can also assign the Group/Security Tag later from Inventory after devices are added.

Click **Browse** to select a CSV file to upload to IND.

NAT Lookup Table

IND uses a Network Address Translation (NAT) lookup table to provide translation between private and public IP addresses. The lookup table is a Comma-Separated Values (CSV) file that you can create and upload to the system prior to device discovery. This allows IND to discover endpoint devices in a NAT network topology. When IND receives a link up trap from the connected switch, IND translates the private host IP address in the trap received to a public IP using this NAT lookup table and discovers the device using the public IP address.

Note the following when using NAT Lookup Table:

- The NAT Lookup Table must be uploaded before Switch Discovery for IND to populate the MAC address for the switch.
- When a new file with NAT mapping information is uploaded to IND, it will override the existing NAT mapping information.
- The Access Profile used for the switch discovery needs to have the protocols of the connected device enabled.
- The neighbor discovery protocols on the switch that IND uses (LLDP, CDP, MAC and ARP, depending on the applicable protocol) must return accurate information.

To use NAT Lookup Table:

1. Click the link **Nat_Lookup_Table_Template.csv** under the Import: section of the page to download the template. Enter the IP address information in the columns provided:
 - Network Range—must not have duplicates or values overlapping with another range.
 - Endpoint Private—must contain the network prefix of the private subnetwork (for example, 192.168.0.0 in the case of 192.168.0.0/24).
 - Endpoint Public—must contain the Network prefix of the public subnetwork (for example, 10.64.0.0 in the case of 10.64.0.0/21).

A maximum of 500 rows can be present in the CSV file.
2. Click **Browse** to select the file with the NAT mapping information, and then click **Upload**.
3. Click **Download** to export the contents of the NAT Lookup Table from IND.

Device Replacement

Whenever IND receives a linkup trap from a switch, it proceeds to discover the neighboring device that is connected to the switch. Before discovery or when adding a device to its inventory, IND checks if there is an existing device with the same IP address, MAC address, or serial number. If there is one, IND does not perform discovery, or it fails to add the device to its inventory.

If you have an existing device that is faulty, you might want to replace the device with another device in the network. Previously, you had to manually delete the existing device and add a new device. Now, IND will autonomously replace a device by deleting the existing device in its inventory and adding a new device when the conditions listed in the following table are met.



Note Device replacement is performed only during linkup trap triggered discovery. Replacement applies only to endpoint devices, not switches.

Device tracking (IPDT) must be enabled on all the ports of the switches and should be up to date. IP traffic from the endpoint is necessary for the switch to update the device tracking table. Refer to the documentation for your switch for information on how to enable device tracking.

IND continues to add new devices according to the existing topology discovery flow for linkup traps when condition number 4 shown in the table below is met.

Table 4: Conditions for Device Replacement

Condition No.	IP Address	MAC Address	Connected Port	Action
1	IP address exists in database	New MAC address	Same switch/port	Delete existing device last seen on port, add new device
2	New IP address	New MAC address	Same switch/port	Delete existing device last seen on port, add new device

Condition No.	IP Address	MAC Address	Connected Port	Action
3	New IP address	Same MAC address	Irrespective of port	Delete existing device irrespective of port, add new device
4	New IP address	New MAC address	No device exists on same switch/port	Add as new device (this is the default linkup discovery flow)



Note For multiport devices with each port having a unique MAC address/IP address, IND deletes the old device in its inventory if it finds another device with a different port/MAC address but the same serial number.

Expected Behavior for Device Replacement

The following is expected behavior for device replacement:

- Device replacement is performed only during linkup trap triggered discovery.
- Only endpoints are replaced and not switches.
- The existing topology discovery flow for link-up trap is maintained.
- Tags of an existing device (before deletion) are assigned to the new device.
- The new device is added under the same group where the old device (before deletion) was present.
- The access profile of an existing device (before deletion) is used for discovery of the new device if it is different from the access profile used for switch discovery.
- IND maintains the same licensed state (licensed or unlicensed) of the new device as the old device (before deletion).
- IND rediscovers a backplane device and its modules after replacement.
If a module is not removed physically from the backplane, IND will still show the module in its inventory because it will be reachable through other modules in the backplane chassis.
- Upon deletion of a backplane device, IND does not delete the devices that are discovered through backplane bridging, if any are found in its inventory. In such cases, you need to manually delete all the devices that were discovered through backplane bridging.
- IND does not replace an existing device if there is any ambiguity.
- Audit trails are captured for device replacements.
- All the information related to a linkup triggered discovery operation is logged in a file under <logDir>/linkupLogs. The file name format of each file is <Switch_IP>_<Short_Port_Name>_<TimeStamp>.log
- New device replacement in topologies including DLR, PTP, REP, PRP, MRP, or any arbitrary ring is not officially certified or supported.

Fallback Mechanism for Obtaining MAC Address

If IND cannot use any of the protocols selected in the access profile to obtain the MAC address for an endpoint device, IND can still get the MAC address by discovering the switch along with the endpoint device as part of a single IP scan. Discovering the endpoint device alone does not obtain the MAC address.

IND also uses this fallback mechanism to determine connected devices.

The fallback mechanism can also be triggered by re-discovering the switch if the endpoint is already discovered. The fallback mechanism is triggered by default for all linkup trap triggered discoveries.

Device Replacement Prerequisites

The following prerequisites must be met for IND to replace a device in its inventory.

- Traps must be properly configured to reach IND.
- Switches must be in the licensed state to process the traps.
- If the switches and endpoint devices are located behind a NAT network, you need to upload a [NAT Lookup Table](#) prior to discovery of switches.
- MAC address resolution and ARP cache entries must be updated accurately.
- Device tracking (IPDT) must be enabled on all the ports of the switches and should be up to date. IP traffic from the endpoint is necessary for the switch to update the device tracking table. Refer to the documentation for your switch for information on how to enable device tracking.
- IND must be running continuously to reflect the latest changes on the network. If IND is not in sync with the network, devices may not be replaced accurately.

If IND has not been running for a while, synchronize IND with the network as follows:

1. Discover all remaining devices that are not in the IND inventory.
 2. Remove all devices from the inventory that are not in the network.
 3. Trigger a topology discovery.
- Connected devices must be populated in IND for endpoint devices. Connected devices may not appear if the endpoint devices are discovered separately. In such cases, trigger a topology discovery or discover the endpoint devices along with the switches.
 - Daisy chain topology is not supported unless LLDP is enabled on the switch.
 - The module of the backplane chassis that was replaced and the new module replacing the old one should be connected to the switch and be directly reachable from IND.
 - If you restore a backup, you must re-discover devices manually and synchronize it with the network.

Guidelines and Limitations

Note these guidelines and limitations for device replacement:

- If a device replacement fails, manually delete the devices that are not in the network from IND and trigger a topology discovery again. This will synchronize IND with the network.
- A switch may not update its ARP cache and device tracking entries if there is no IP traffic seen from the endpoint device. Without device tracking entries, IND cannot accurately replace a device.

- If there is a new IP address assigned to a device, ISE will have 2 entries after device replacement: one entry with the old IP address and another entry with the new IP address. This is even after IND sends a delete notification for the device with the old IP address. This is the default behavior of ISE.
- It might take 2-8 minutes for IND to complete the device replacement after it receives the trap.
- If the new IP address is un-reachable, IND still deletes the old device in its inventory. In such cases, you should resolve the reachability issues and discover the new device by generating the trap again (re-connecting the device to the switch).
- The information that IND collects from the device might vary according to the protocols that are selected in the access profile and those that are configured on the device.
- If IND detects a daisy chain topology (multiple MAC addresses seen on the same port of a switch for which a linkup trap is received), IND logs an error and does not perform device replacement. You need to dismantle the daisy chain topology or enable LLDP, manually re-discover the topology, and try generating a linkup trap again.
- If a CIP module is not physically removed from a backplane chassis, the module is still reachable through other modules with a reachable IP address. In such cases, IND will add the module again after deletion when it refreshes the backplane chassis in its inventory.

Inventory

The **Operate > Inventory** page displays all the devices that the system discovered from a scan of the network. See [Discovery, on page 24](#) for more information about network scans. See [Device Prerequisite Configuration, on page 76](#) for the device configuration required for the system to successfully discover Industrial Ethernet (IE) switches.



Note The Inventory page displays devices based on the Context Group drop-down menu selection. The Context Group drop-down menu lists the groups and subgroups that you can access based on your group assignment. See [Buttons and Controls, on page 123](#) for information about the Context Group menu.

The Asset Inventory is organized into the following categories, shown on the left in Device Filters:

- [Licensed Devices, on page 40](#): Displays the devices listed in the [Device Pack](#). Licensed devices can be managed by the system. The device types in this category include:
 - IE and Stratix switches and CIP devices (EtherNet/IP nodes).
 - CIP devices that are DLR Supervisor capable.
 - CIP devices that are PRP capable.
 - Profinet Siemens PLC devices that are MRP capable.

CIP devices use backplane bridging to route CIP messages (at the application level) across the backplane of a Programmable Logic Controller (PLC). CIP messages arrive on one communication adapter and are sent on another communication adapter. IND can discover devices connected behind a PLC. CIP devices are described further in [Licensed Devices, on page 40](#) and [Licensed Device Details - CIP Device, on page 69](#).

The Licensed Devices category also includes partial information about Licensed Devices for which SNMP failed, but protocols such as CIP, PROFINET or MODBUS identified the device. These devices have Error Status set as SNMP Failure. They cannot be moved to Licensed state.

- [All Devices, on page 46](#): Displays devices in the Licensed Devices category as well as the following other devices:
 - CIP, BACnet, MODBUS, PROFINET, and OPC UA automation devices connected to Licensed Devices that are in Licensed state.
 - Windows hosts connected to Licensed Devices that are in Licensed state.
 - SNMP devices that are not managed by the system.
 - All other devices that are not recognized by the system.

You can perform these actions on the Inventory page:

- Filter the devices to display by selecting one or more device filters on the left of the page.

In addition to filtering by Category, you can filter devices by Groups, Device Type, Features, Protocol, State, and Vendor.



Note To view only manually added devices, filter the devices by selecting the State as "Not Supported."

- To view device-specific details, click the name of the device from the Licensed Devices or All Devices categories in the table. See [Device Details, on page 48](#) for more information.
- To export a Comma Separated Values (CSV) or Excel file of inventory assets and their attributes, click



on the right of the Inventory page. In the Export Inventory pop-up window, select the System and Asset attributes to include, and then click **Download CSV** or **Download Excel** to download the file to your local system.

- Select devices from the list and click **With Selected** to perform the following actions in the With Selected Devices pop-up window:
 - To delete a device, click **Delete**.
 - To change the administrative state of the selected Licensed device(s), select the state from the **Change License State** drop-down list. See [Licensed Devices, on page 40](#) for more information about changing the License State.



Caution The system makes configuration changes to a Licensed IE device that is moved to Licensed state by loading a bootstrap configuration to the device. See [Bootstrap Configuration, on page 78](#) for information about the bootstrap configuration before proceeding with administrative state changes.

- To add or remove a tag association for the device, click **Regular** or **Security**, select up to five regular tags or one security tag from the drop-down list, and then click **Add** or **Remove**.

For information about tags, see [Tags, on page 115](#).

Licensed Devices

Licensed Devices can have an administrative state (see State in table below) of Licensed or Unlicensed. The administrative state of a Licensed device must be set to **Licensed** for the system to manage the device.

The state of a device in the inventory reflects the *management state* of the device from the perspective of the system, and has no bearing on the current *operational state* of the device.

Newly discovered Licensed devices are added to the asset inventory in the Unlicensed state. Although the system does not monitor these devices, it may connect to these devices and collect information to keep the asset inventory up to date. All incoming traffic (such as SNMP traps) from the device are ignored. Only devices in the Unlicensed state can be deleted from the asset inventory. Licensed Devices may be moved to the Unlicensed state either manually by a user with Device Management privileges, or automatically by the system due to device license violations.

The system operates as follows in Classic Licensing when you move a device from the Unlicensed to Licensed state:

1. The system verifies that you have sufficient licenses available (1 license per device).
2. If no licenses are available, you are informed that devices did not move to the Licensed state because licenses were not available, and a state change task is not triggered.
3. If not enough licenses are available, (for example, you submitted a state change request for 10 devices and only 5 licenses are available), you are informed that only some of the devices (in this example, 5) will be moved to the Licensed state due to insufficient number of licenses. Devices are randomly picked and the state change task is submitted for only those devices.

IE Switch Move to Licensed State

When an IE switch is moved to the Licensed state, the system loads the device with a [Bootstrap Configuration, on page 78](#) so that it can be monitored. The system periodically polls these devices to collect metrics. SNMP traps originating from these devices are processed by the system and annunciated as Alarms.



Note After the bootstrap configuration is erased from the device, for example, when a device is reset, IND cannot collect information from the device until you move the device to the Unlicensed state and back to the Licensed state again. During this transition, IND pushes the bootstrap configuration necessary for it to communicate with the device.

CIP Device Move to Licensed State




CIP devices are licensed based on feature (see description of the Features field in the Licensed Devices table below). CIP devices that support the backplane bridging feature and that are moved to Licensed state perform backplane bridged discovery on all communication modules. Discovery is performed by browsing the subnet of the ports on that module. During this discovery, only the subnets at the module levels are browsed. If another CIP multi-IP device is found, it is discovered as another Unlicensed device. Move the Unlicensed CIP device to the Licensed state, then trigger backplane discovery on the device as described in [Licensed Device Details - CIP Device, on page 69](#).






Note If a CIP device in Licensed state is changed to Unlicensed due to insufficient licenses or some other user operation, you lose the ability to refresh information about devices in the backplane bridged network.

Table 5: Licensed Devices Table


Alarm Status	Severity of alarms for the device.
Name	Textual description of the device. + preceding the device name indicates that this is a CIP device (EtherNet/IP Node). CIP devices have a chassis made up of slots containing communications adapters. Click + to display a pop-up with information about the slots (see table below for descriptions).
Protocol	Protocol of the Licensed device: <ul style="list-style-type: none"> • CIP—EtherNet/IP node • MULTIPROTOCOL— System-defined value for supported network devices that use multiple protocols such as SNMP, SSH/TELNET, WSMA (HTTP/HTTPS), or JSON-RPC (HTTP/HTTPS) for the system to discover and manage these devices.
State	Administrative state of the device: <ul style="list-style-type: none"> • Licensed—The system actively manages devices that are in Licensed state. Devices in Licensed state consume a device management license. • Unlicensed—This state refers to devices that can be licensed but have not been moved to Licensed state. The system does not manage devices that are in Unlicensed state. Devices in Unlicensed state do not consume a device management license.
IP Address	Internet address of the device in dot-decimal notation.
MAC Address	The device MAC address.

Connected To	<p>Names of the devices that this device is connected to. This column is empty if the device has no connected devices.</p> <ul style="list-style-type: none"> • Click the link to display a pop-up window that contains the list of connected device names and may also contain the port names. • Click the connected device name link to display the device details, if that device has been discovered by the system. For Licensed Device ports only, click the port name link to display port details.
Product ID	Asset tracking identifier of the device.
Group	Concatenation of all names in the unique path from root to the parent of the group, separated by ">".
Tags	<p>The tags associated with this device.</p> <ul style="list-style-type: none"> • If tags are associated with this device, the tag names are displayed as a link. Click the link to display the Associated Device Tags pop-up window to add or remove tags. • If no tags are associated with the device, + is displayed as a link. Click the link to display the Associated Device Tags pop-up window to add or remove tags.
Serial Number	<p>(not displayed by default; click  to change table display options)</p> <p>Vendor-specific serial number string for the device.</p>
Description	<p>(not displayed by default; click  to change table display options)</p> <p>The description of the device obtained from the device during discovery or that you update by using the Update Device button or when you add a device manually.</p>
Vendor	<p>(not displayed by default; click  to change table display options)</p> <p>Name of the manufacturer of the device.</p>

Software Version	<p>(not displayed by default; click  to change table display options)</p> <p>Software revision string for the device.</p>
License Expired	<p>(not displayed by default; click  to change table display options)</p> <p>Shows whether license is expired.</p>
Device Access Profile	<p>(not displayed by default; click  to change table display options)</p> <p>The Device Access Profile used to discover the device.</p>

Features	
----------	--




(not displayed by default; click  to change table display options)

Features supported by IND and that are supported and currently enabled on licensed devices:

- Backplane bridging: IND can discover devices that are attached to the PLC.
- Device Level Ring (DLR): IND gets DLR ring participants, monitors the DLR ring and gets information about the health of the ring, generates an alarm when there is a fault on the device, and shows DLR ring information on the topology overlay.
- Media Redundancy Protocol (MRP): IND gets MRP ring participants, monitors the MRP ring and gets information about the health of the ring, generates an alarm when there is a fault on the device, and shows MRP ring information on the topology overlay.
- Parallel Redundancy Protocol (PRP): IND gets PRP network participants, monitors the PRP network and gets information about the health of the network, generates an alarm when there is a fault on the device, and shows PRP information on the topology overlay.
- Precision Time Protocol (PTP): IND gets PTP clock information including PTP master and PTP grandmaster, monitors the device to track clock master and grandmaster changes, generates an alarm when there is a change that will affect the system time, and shows PTP clock distribution information on the topology overlay.
- Resilient Ethernet Protocol (REP): IND gets REP segment information for the switch, segment members, and segment interfaces, monitors the REP segment nodes and gets information about the health of the REP topology, generates an alarm when there is a fault on the device, and shows REP information on the topology overlay.

Note If a feature is configured on a device after it is licensed, you need to perform an on-demand device refresh to obtain the feature configuration. Click **Retrieve Device Data** (switches) or **Refresh CIP Device Data** (CIP devices) on the Details

	page for the device to refresh the data.
Roles	<p>(not displayed by default; click  to change table display options)</p> <p>Shows the role of the device for the features listed above when the feature is supported and currently enabled on the device. Shows "Disabled" if the feature is supported but not currently enabled.</p>



The following information appears in a pop-up when you click + in front of a CIP device name.

Table 6: Communication Module(s) Table

Slot	Communication module slot number.
Device Profile	Standard device classification that defines the capabilities and characteristics of this CIP device.
Revision	Revision number of the CIP device.
Serial Number	Vendor-specific serial number string for the CIP device.
Product Name	Vendor-specific product name of the CIP device.
IP Address	The IP address assigned to the port of the CIP module.

All Devices

Alarm Status	Severity of alarms for the device.
Name	Textual description of the device.
Device Type	Type of device (for example, EtherNet/IP Node).
Protocol	Protocol of the device.
IP Address	Internet address of the device in dot-decimal notation.

Connected To	<p>Names of the devices that this device is connected to. This column is empty if the device has no connected devices.</p> <ul style="list-style-type: none"> • Click the link to display a pop-up window that contains the list of connected device names and may also contain the port names. • Click the connected device name link to display the device details, if that device has been discovered by the system. For Licensed Device ports only, click the port name link to display port details.
Product ID	Asset tracking identifier of the device.
Group	Concatenation of all names in the unique path from root to the parent of the group, separated by ">".
Tags	<p>The tags associated with this device.</p> <ul style="list-style-type: none"> • If tags are associated with this device, the tag names are displayed as a link. Click the link to display the Associated Device Tags pop-up window to add or remove tags. • If no tags are associated with the device, + is displayed as a link. Click the link to display the Associated Device Tags pop-up window to add or remove tags.
Vendor	Name of the manufacturer of the device.
Serial Number	<p>(not displayed by default; click  to change table display options)</p> <p>Vendor-specific serial number string for the device.</p>
Description	<p>(not displayed by default; click  to change table display options)</p> <p>Description of the device.</p>

The following information appears in a pop-up when you click + in front of a CIP device name.

Table 7: Communication Module(s) Table

Slot	Communication module slot number.
------	-----------------------------------

Device Profile	Standard device classification that defines the capabilities and characteristics of this CIP device.
Revision	Revision number of the CIP device.
Serial Number	Vendor-specific serial number string for the CIP device.
Product Name	Vendor-specific product name of the CIP device.
IP Address	The IP address assigned to the port of the CIP module.

Device Details

To view details about a device, select the device category in the left pane of the **Operate > Inventory** page and then click on the device name in the table. You can also click the device name link displayed in the pop-up panel on the right when the device is selected in the **Operate > Topology** map. Details available for a device depend on the administrative state of the device (Licensed, Unlicensed, or Not Applicable) and the device type.

Licensed Device Details - Switch

Details for Industrial Ethernet (IE) switches include the physical aspects of the device, inventory and metric data, configured network interfaces, and VLANs associated with network ports.

If the device is in Unlicensed state, the Licensed Device details page displays a link to move the device to Licensed state.

- Click **View Topology** to open the Topology page with the device selected.
- Click **Open Device Manager** to launch the Device Manager application on the device. You must have a Device Manager user name and password.
- Click **Retrieve Device Data** to get current values for all the information collected from the device.
- Click **Update Device** to manually update Name and Description fields.

You may want to manually update these fields for the discovered devices with protocol as MULTIPROTOCOL (IE and Stratix switches), for example, if you want to add a custom value for the fields. If you do not specify a value for the Name field, the default is the hostname or IP address returned by the device at discovery. The value for Name is sent as the Asset Name for a device to ISE through pxGrid.

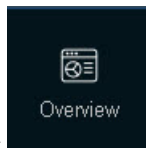


Note Manually updated field values take priority over periodic updates. That is, the manually updated value will not be overwritten with the data fetched from the device during periodic data refresh. After you update an attribute for a device, it will never be updated by periodic data refresh from the device until the device is deleted and re-discovered.

Manually updated fields are flagged in the Device Overview with an "Edited" label.

- Click the menu tiles on the left of the page (described below) to view information about the device.

Overview




Click the **Overview** menu tile on the device details page of a licensed switch to view comprehensive status and information about the device:

- If there are any alarms for the device, a banner at the top of the page shows the total alarm count for this device and the most recent alarm with the highest severity. The banner shows the type, message, generated time, and severity for that alarm—red (critical), orange (major), or yellow (minor). Click **View List** to see all the alarms for this device. Click **View Details** to display detailed alarm information.
- Health—Status of the device hardware, such as temperature and CPU usage.
- Bandwidth—Chart of bandwidth utilization on the device. Click **1 Hour**, **1 Day** or **1 Week** to select the time scale of the chart. Click the blue, red, or green box to select the type of utilization to display (Rx, Tx, or Avg). Click **View Details** to view the chart in a pop-up window and select a specific time period.
- Recent Activity—Audit Trails entries for this device. Click **View Details** to see the list on the **Operate > Audit Trails** page.
- Physical Device View—Graphic representation of the device that shows LED and port status. Click on a port in the image to display port details or change port settings (see [Port Settings, on page 49](#)).
- Device Overview—Information about the device such as Name, Host Name, IP Address, Product ID, Serial Number, etc.



Note The Name field is set to the host name or IP address of the device by default, but you can click **Update Device** on the Details page to set a custom name. However, the Host Name field will always indicate the host name value from the device.

Click  next to Software Version to install the software image on the device. In the Install Software Image pop-up window, select from eligible images and then click **Install**. Eligible images must be previously uploaded to the system using the **Maintain > Software Images** page (see [Software Images, on page 93](#)).

Port Settings

When you click on a port in the Physical Device View, a pop-up window appears with information about the port and settings that you can change. To change port settings, the device must be in Licensed state, and you must have Port Settings permission. (System Administrator, Network Administrator, and Operator roles inherit this permission by default.)




Note The available settings and values for a port depend on the device. Port speed and duplex mode are combined into one setting for IE 1000 switches.

Only RJ-45 ports are supported for configuration. SFP and dual-purpose ports are not supported.

Do not change settings (for example, shut) on a port required for communication with IND . Configure the commands that you want to set on the device.

You can change port settings for only one port at a time. Click **Save** to submit the changes.

The system implements the requested port settings changes as a task. The task must be completed before you

can make another change on the same port. To view the status of the change, click  on the upper right to display the Tasks page. The system automatically refreshes the device data.



Note Shutting down a port may take some time to complete. Wait approximately 1 minute so that IND can retrieve steady state information from the device and refresh the data.

Table 8: Port Settings

Name	(not editable) The port type and port number, for example, FastEthernet1/4. Click the link to display the Port Details, on page 75 page.
Description	Optional description of the port for reference.
Speed	Select the operating speed from the drop-down list: <ul style="list-style-type: none"> • Auto-speed—Allows a connected device to negotiate the link speed. • 10Mb/s • 100Mb/s
Duplex	Select the duplex setting from the drop-down list: <ul style="list-style-type: none"> • Auto-duplex—The connected device can negotiate the duplex setting with the switch. • Half-duplex—The connected device must alternate sending or receiving data. • Full-duplex—Both devices can send data at the same time.

Access VLAN	(applicable only to Access ports) Select the Access VLAN from the drop-down list. The Access VLAN is the VLAN that an interface belongs to and carries traffic for, when the link is configured as an access port.
Admin Mode	(not editable) The administrative mode of the port, for example, access or trunk.
Operation Mode	(not editable) The operational mode of the port, for example, down.
Disable/Enable	Click the green toggle button to disable (shut) or enable (no shut) the port.

Connected Devices

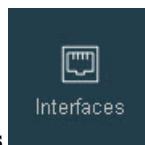


Click the **Connected Devices** menu tile on the device details page of a licensed switch to display information about the devices connected to this device. Click on a device or port name in the Connected Device(s) table to display details for the connected device or port. (See [Port Details](#), on page 75 for information about the Port Details page.)



Note Links are shown only for the devices in your Auth Group and subgroups. For other devices, the links are disabled.

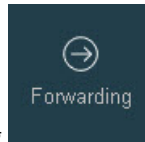
Interfaces



Click the **Interfaces** menu tile on the device details page of a licensed switch to display detailed information about the interfaces on the device:

- The **Ports** tab displays detailed port information. Click on a port name in the Port(s) table to display details for the port.
- Click the **L2 Interfaces** or **L3 Interfaces** tab to view interface settings and status.
- The **PoE** tab shows details for Power over Ethernet interfaces on the device, including the total power available and used, the power allocated to interfaces, and PoE status.

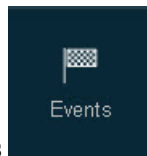
Forwarding



Click the **Forwarding** menu tile on the device details page of a licensed switch to display the MAC address table of MAC addresses that the device learns from interfaces. On every collection, all existing entries in the table are deleted, and new entries are created. Click on a port name under Port Resource to display details for the port.

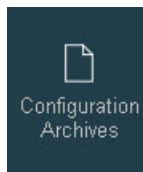
Click the **VLANs** tab to see a list of all the VLANs configured on the device.

Events



Click the **Events** menu tile on the device details page of a licensed switch to display event details for the device. Event details include the event type, the message about the event, the time stamp of the event, and associated port, if applicable. Events include device alarms and notifications.

Configuration Archives



Click the **Configuration Archives** menu tile on the device details page of a licensed switch to display the Configuration Archive(s) for the device.

- Click the link under Backup Time to display the contents of the Configuration Archive.

If there is more than one backup for the device, you can check the **Base Version** check box in the Config Archive Content pop-up window to make the selected configuration backup the Base Version.

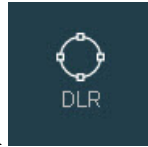
- Click **Backup Now** to perform an on-demand backup of the device configuration.



- Click the Restore icon to restore a backup configuration.
- Select two configuration archives, click **With Selected**, and then click **Configuration Diff** to display a side-by-side comparison of the two backup configurations.

See [Configuration Archives, on page 90](#) for more information about Configuration Archives.

DLR



Click the **DLR** menu tile on the device details page to display Device Level Ring (DLR) parameters and statistics for a DLR node. DLR information is available when the DLR feature is supported and enabled on a licensed device.

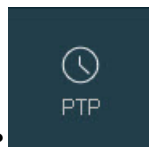
The information is refreshed every 15 minutes. To change the frequency at which this information is updated, change the data collection timing for metrics status poller under the **Settings > System Settings > Data Collection** page.

If the device is a node in more than one ring, click the tab for the ring you want to view. Information includes role, network status, IP and MAC addresses, list of ring members, Active Supervisor parameters, and fault statistics.

Overview	
Mode	Mode of the DLR device: Ring Node, Active Supervisor, or Backup Supervisor.
Network Topology	Ring
Network Status	<p>Current network status based on the device's view of the network. Possible values are:</p> <ul style="list-style-type: none"> • Normal—Operation is normal. • Ring Fault— A ring fault has been detected. • Unexpected Loop Detected— A loop has been detected in the network. • Partial Network Fault— A network fault has been detected in one direction only. This fault occurs only when the node is the active ring supervisor. • Rapid Fault/restore Cycle— A series of rapid ring fault/restore cycles has been detected. <p>Similar to the Partial Network Fault status, the supervisor remains in a state with forwarding blocked on its ring ports.</p>
IP Address	IP address of the ring node.
Revision	Revision of the DLR protocol running on the device.
MAC Address	MAC address of the ring node.
Ring Participants	
Number	Number of the ring participant.
MAC Address	MAC address of the ring participant.

IP Address	IP address of the ring participant.
Device	Device name of the ring participant. Click the link to go to the details page of the device. Note Links are shown only for the devices in your Auth Group and subgroups. For other devices, the links are disabled.
Role	Role of the ring participant: Ring Node, Active Supervisor, or Backup Supervisor.
Status	Status of the ring participant.
Ports	
Port 1	Name of DLR ring port 1.
Port 2	Name of DLR ring port 2.
Active Supervisor Parameters	
MAC Address	MAC address of the active supervisor.
IP Address	IP address of the active supervisor.
Precedence	Precedence value assigned to ring supervisor and transmitted in beacon frames.
Redundant Gateway Parameters	
Redundant Gateway Status	Status of the Redundant Gateway: Active Gateway or Backup Gateway.

PTP



Click the **PTP** menu tile on the device details page to display information about Precision Time Protocol (PTP) on the device. PTP information is available when the PTP feature is supported and enabled on a licensed device. Because the root of PTP timing distribution is the grandmaster, the topology view is only available if the grandmaster is discovered and licensed in IND.

Click the tab to view PTP details for the device or to view PTP domain information. Domain summary information is available for all domains configured for the given device. If the device is a chassis and the modules in the chassis belong to different domains, then there is one summary tab per domain. Domains are identified by the domain number displayed on the tab.

The domain summary consists of a list of grandmaster capable devices and their configured precedence. This list contains only licensed devices in the domain.

Table 9: PTP Details

Overview	
Time Synchronized	Displays whether the local clock is synchronized to a master.
System Time	Current time as measured by the system clock.
Clock Type	<p>The PTP clock type of this device:</p> <ul style="list-style-type: none"> • Grandmaster: The highest-ranking clock within its PTP domain and is the primary reference source for all other PTP elements. • Slave clock: Receives the time information from a master clock by synchronizing itself with the master clock. It does not redistribute the time to another clock. • Ordinary clock: A PTP clock with a single PTP port. It can be a master clock (grandmaster) or a slave clock. • Boundary clock: Intermediary device between a PTP grandmaster and its PTP slave clients. It has multiple PTP ports in a domain and maintains the time scale used in the domain. Different ports on the boundary clock can be master ports or slave ports. The boundary clock terminates the PTP flow, recovers the clock and timestamp, and regenerates the PTP flow. A slave port recovers the clock and master ports to regenerate the PTP packets. • Transparent clock: Measures the time needed for a PTP event message to transit the device and then compensates for the packet delay. Note that a transparent clock does not get its system time from the grandmaster, so a transparent clock type is labeled on the topology map but the timing distribution link is not shown.
Last Updated	Timestamp of the last PTP information update.
PTP Domain Number	A number that identifies a group of devices that synchronize to each other using the PTP protocol.
Grand Master Clock, Master Clock, Local Clock	

Grandmaster, Master	<p>(Grandmaster and Master Clock only)</p> <p>Name of the Grandmaster or Master clock.</p> <p>Click the link to go to the details page of the device if the device is discovered and licensed in IND.</p> <p>Note Links are shown only for the devices in your Auth Group and subgroups. For other devices, the links are disabled.</p>
Hardware Revision	Device hardware version number.
Manufacturer Name	Manufacturer of the device.
Model	The device model number.
UTC Offset	Offset between the International Atomic Time (TAI) and Coordinated Universal Time (UTC) in seconds.
Time Property Flags	<p>16-bit word that specifies the time properties of the clock. Time properties and bit index are:</p> <ul style="list-style-type: none"> • Leap indicator 61: 0 • Leap indicator 59: 1 • Current UTC offset valid: 2 • PTP timescale: 3 • Time traceable: 4 • Frequency traceable: 5 <p>For example, 4 is 0101 and means that leap indicator 61 is set and current UTC offset is valid.</p>
Offset Threshold From Grandmaster	<p>(Grandmaster Clock only, when Grandmaster is licensed)</p> <p>Click the link to set the offset threshold value in nanoseconds. The range is 0 to 6e+ 11. Setting the value to 0 resets the threshold. The default is 0 (no threshold is set and no alarm is generated).</p> <p>Any PTP node under this grandmaster generates an alarm when this threshold is exceeded. The alarm is cleared when the offset falls below the threshold.</p> <p>Note You cannot set the offset threshold value on a boundary clock device. If you set the offset value for the grandmaster in the PTP domain and the grandmaster changes, the system moves the threshold to the new grandmaster automatically.</p>

Offset from Grand Master	(Local Clock only) Time difference between the master clock and the local slave clock, measured in ns.
Offset from Master	(Local Clock only) Time difference between the grandmaster clock and the local slave clock, measured in ns.
Identity	MAC address or a complete EUI-64 value that identifies the clock in the PTP network.
Class	Represents a relative measure of the clock quality used by the Best Master algorithm to determine the grandmaster. The class is a value between 0 and 255, with 0 as the best clock.
Accuracy	Specified as a graduated scale starting at 25 ns and ending at greater than 10 seconds or unknown. A GPS time source will have an accuracy of approximately 250 nanoseconds. A HAND set clock will typically have accuracy less than 10 seconds. The lower the accuracy value, the better the clock.
Variance	Variance measure of clock quality used by the Best Master algorithm to determine the grandmaster. The value is represented in offset scaled log units. The lower the variance, the better the clock.
Source	Time source (for example, atomic clock or GPS) used by the grandmaster clock.
Priority 1	(Grand Master Clock only) User-assigned priority of each clock. The priority overrides the default criteria (class, accuracy, and variance) for the most accurate master clock selection. The value is between 0 and 255. The highest priority is 0.
Priority 2	(Grand Master Clock only) User-assigned priority of each clock. Specifies the Best Master ranking of this clock after clock quality (class, accuracy, and variance) has been evaluated and supersedes the tie-breaker. This attribute allows the user to override the automatic selection of the best master clock after quality measures have been evaluated; that is, choose the best master from a set of clocks of equal quality. The value is between 0 and 255. The highest priority is 0.
PTP Ports	

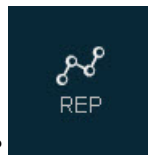
Port Name	Name of the PTP port on the device.
Port State	State of the PTP port: <ul style="list-style-type: none"> • Initializing • Faulty • Disabled • Listening • Pre-Master • Master • Passive • Uncalibrated • Slave
Grand Master Clock History, Master Clock History	
Number	Clock order, from newest to oldest.
Clock Identity	MAC address or a complete EUI-64 value that identifies the clock in the PTP network.
Clock Node	Device name.
Time Stamp	Time at which clock information was updated in IND.

Table 10: Domain Summary

Rank	Displays the current grandmaster as 1, followed by the other grandmaster capable nodes ranked according to the probability of the node becoming grandmaster if the current grandmaster node goes down. Note The Clock rank is calculated based on information available in IND. If all devices are not discovered and licensed in IND, this rank might be incorrect.
Device	Device name of the node in the PTP domain. Click the link to go to the details page for the device. Note Links are shown only for the devices in your Auth Group and subgroups. For other devices, the links are disabled.
PTP Role	Role of the device in the PTP domain.
Product ID	Asset tracking identifier of the device.

Precedence 1	User-assigned priority of each clock. The priority overrides the default criteria (class, accuracy, and variance) for the most accurate master clock selection. The value is between 0 and 255. The highest priority is 0.
Precedence 2	User-assigned priority of each clock. Specifies the Best Master ranking of this clock after clock quality (class, accuracy, and variance) has been evaluated and supersedes the tie-breaker. This attribute allows the user to override the automatic selection of the best master clock after quality measures have been evaluated; that is, choose the best master from a set of clocks of equal quality. The value is between 0 and 255. The highest priority is 0.

REP



Click the **REP** menu tile on the device details page to display the collected REP information. REP information is available when the REP feature is supported and enabled on a licensed device.

The information is refreshed every 30 minutes, the default inventory status data collection period. To change the frequency at which this information is updated, change the data collection period for metrics status poller under the **Settings > System Settings > Data Collection** page.

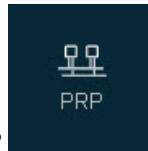
Overview	
Bridge MAC	PortFast Bridge Protocol Data Unit (BPDU) class MAC address to which REP packets are sent.
Admin VLAN	REP administrative VLAN for REP to transmit hardware flood layer (HFL) messages.
Port Details	
Name	Port type and number.
Port ID	REP port identifier, formed by appending the port priority and port number to the bridge MAC address.

Port State	<ul style="list-style-type: none"> Failed: A port configured as a regular segment port starts as a failed port. Alt: After neighbor adjacencies are determined, the port transitions to the alternate port state, blocking all VLANs on the interface. Blocked port negotiations occur, and when the segment settles, one blocked port remains in the alternate role, and all other ports become open ports. Open: When a failure occurs in a link, all ports move to the failed state. When the alternate port receives the failure notification, the port changes to the open state forwarding all VLANs.
Operational Status	<p>Current operational link state of the REP port:</p> <ul style="list-style-type: none"> initDown—Initial REP link state. If a REP configured interface is down, it is in the initDown state. none—REP is not operational on the interface. noNeighbor—REP is yet to discover its neighbor. oneWay—Messages have been received from the neighbor but the link has not been declared to be twoWay yet. twoWay—REP is fully operational. flapping—There is a mismatch in the received port information (either local or remote) for the neighbor. wait—Forced transient state before REP starts discovering its neighbor. Unknown—The link state cannot be determined.
LSL Ageout Timer	REP link status layer (LSL) ageout timer value.
Preferred Flag	Indicates that the port is the preferred alternate port or the preferred port for VLAN load balancing.
STCN Propagate To	Specifies the interface to which the REP edge should propagate the segment topology change notifications.
Segment Details	
Segment	
MAC Address	Bridge MAC address.
Port Name	Port type and number.

Device	Name of the REP device.
Role	<p>Role of the port in the REP segment:</p> <ul style="list-style-type: none"> • Primary Edge—Participates in VLAN load balancing. • Primary Edge No-Neighbor—Primary edge with no external REP neighbor on a port. • Secondary Edge—Acts as secondary edge port in the segment. • Secondary Edge No-Neighbor—Secondary edge with no external REP neighbor on a port. • Intermediate—a port forwarding traffic only for a subset of VLANs, for the purpose of VLAN load balancing.
Status	<ul style="list-style-type: none"> • Failed: A port configured as a regular segment port starts as a failed port. • Alt: After neighbor adjacencies are determined, the port transitions to the alternate port state, blocking all VLANs on the interface. Blocked port negotiations occur, and when the segment settles, one blocked port remains in the alternate role, and all other ports become open ports. • Open: When a failure occurs in a link, all ports move to the failed state. When the alternate port receives the failure notification, the port changes to the open state forwarding all VLANs.
Segment Archive	Displays information about the segment before the last event (for example, a failure) within the segment occurred. See Segment descriptions above.
Load Balancing	
Port Name	Port type and number.

Role	<p>Role of the port in the REP segment:</p> <ul style="list-style-type: none"> • Primary Edge—Participates in VLAN load balancing. • Primary Edge No-Neighbor—Primary edge with no external REP neighbor on a port. • Secondary Edge—Acts as secondary edge port in the segment. • Secondary Edge No-Neighbor—Secondary edge with no external REP neighbor on a port. • Intermediate—a port forwarding traffic only for a subset of VLANs, for the purpose of VLAN load balancing.
Device	Name of the REP device.
Blocked VLAN	Any VLANs blocked by this port for load balancing purposes.
Preempt Delay Timer	Waiting period after a segment port failure and recovery before REP VLAN load balancing is triggered.
Load Balancing Block VLAN	List of VLANs configured to be blocked at the alternate port.
Load Balancing Block Port	<p>Method defined to identify the alternate port in the segment that takes part in VLAN load balancing by blocking a subset of VLANs after preemption:</p> <ul style="list-style-type: none"> • none—No method is specified to identify the alternate port. In this case, the primary edge blocks all VLANs after preemption. • offset—Identifies the port by a number that indicates the offset of the port from an edge port. • portId—Uses the port identifier. • prefer—Selects the port in the segment that is configured as the preferred alternate port for VLAN load balancing.

PRP



Click the PRP menu tile on the device details page to display information about Parallel Redundancy Protocol (PRP) on the device. PRP details are available when the PRP feature is supported and configured on a licensed device.

A PRP channel or channel group is a logical interface that aggregates two Gigabit Ethernet interfaces (access, trunk, or routed) into a single link. In the channel group, the lower numbered Gigabit Ethernet member port is the primary port and connects to LAN-A. The higher numbered port is the secondary port and connects to LAN-B. The PRP channel remains up as long as at least one of these member ports remains up and sends traffic. When both member ports are down, the channel is down. The total number of supported PRP channel groups is 2 per switch, and the interfaces that can be utilized for each group on each switch series are fixed.



Note For more information about PRP, see [Parallel Redundancy Protocol \(PRP\) for IE 4000, IE 4010, and IE 5000 Switches](#) or [Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches](#).

PRP information is refreshed every 15 minutes. To change the frequency at which this information is updated, change the data collection timing for metrics status poller under the **Settings > System Settings > Data Collection** page.

Click **Clear Statistics** to initiate a task for clearing PRP related statistics on the device. On a switch acting as a RedBox, this clears both the channel statistics and node table statistics counters. On an IACS device supporting CIP Object 56 and 57 acting as DAN, this clears only the channel statistics counters. After the Clear Statistics task is completed, refresh the device (click **Retrieve Device Data**) to view updated information.

If the device is configured for more than one PRP channel, select the PRP channel for which you want to view statistics from the drop-down menu.

Overview

Node Name	The selected PRP channel selected, PRP-channel1 or PRP-channel2. For CIP devices, the Node Name can be a custom name which is set on the device.
Role	Role of the device in the PRP network: DAN or REDBOX.
Duplicate Discard	Displays the duplicate packet handling used on the device: Do not Discard or Discard.
Version	PRP version on the device.
Node Type	PRP.
MAC Address	Physical address of the PRP channel interface.

Transparent Reception	Displays the Redundancy Check Trailer (RCT) handling used on the device: Do not Remove RCT or Remove RCT.
Access VLAN ID	For Access mode, the VLAN that the PRP channel interface belongs to and carries traffic for. Note Access VLAN ID is not shown if the PRP channel is in trunk mode or routed mode.
Allowed Trunk VLANs	If the PRP channel interface is in trunk mode, the VLAN Identifiers for which traffic is allowed. Note Allowed Trunk VLANs is not shown if the PRP channel is in access mode or routed mode.

Channel Details

LAN-A, LAN-B	Redundant, active Ethernet networks that operate in parallel and are fault independent.
MAC Address	Physical address of the PRP channel interface.
Interface	Name of the PRP channel interface.
Status	Status of the PRP channel interface: Up (in use) or Down.

Node Details



Note The Node attributes displayed depend on the Device role (REDBOX or DAN).

Nodes	
Revision	Node table revision.
DAN Count	Number of Dual Attached Node (DAN) MAC addresses for the selected channel.
LAN-A Count	The number of devices that are seen on the interface connected to LAN-A and not configured as RedBox or DAN.
Static Entries Count	Number of static entries for this channel.

Node Last Seen Threshold	(Supported devices only) Threshold for the time since the last frame from nodes on the selected channel was received. An alarm is generated when the last seen time exceeds this threshold. The default threshold value is 3 seconds. To change the threshold, click the link, enter a value from 1 - 300, and then click Save .
Maximum Instances	Maximum number of node table instances supported by the device.
Number of Instances	The number of node table instances that the device currently has.
LAN-B Count	The number of devices that are seen on the interface connected to LAN-B and not configured as RedBox or DAN.
MAC Address	Physical address of the PRP node.
Host Name	The device name or IP address as discovered by IND. Click the link to go to the device details page for the device.
Type	The type of the PRP node: RedBox, VDAN, LAN-A (LAN-A switch or SAN switch connected to LAN-A), LAN-B (LAN-B switch or SAN switch connected to LAN-B).
Dynamic	Whether or not (Yes or No) the entry was added as a learned MAC address.
Last Seen LAN-A	Time since the last frame from this node was received over LAN A.
Last Seen LAN-B	Time since the last frame from this node was received over LAN B.
TTL	Aging timestamp for the learned MAC address.
Packets Received LAN-A	Number of packets received on LAN A.
Packets Received LAN-B	Number of packets received on LAN B.
Wrong Packets LAN-A	The number of packets received on LAN A having the wrong LAN A destination.
Wrong Packets LAN-B	The number of packets received on LAN B having the wrong LAN B destination.
VDANs (shown only for PRP Nodes with Role as REDBOX; not shown for DANs)	

Static Entries Count	Number of static MAC addresses for this channel.
MAC Entries Count	Number of MAC addresses (static and dynamic) for this channel.
MAC Address	Physical address of the PRP node.
Host Name	The device name or IP address as discovered by IND. Click the link to go to the device details page for the device.
Dynamic	Whether or not (Yes or No) the entry was added as a learned MAC address.
TTL	Aging timestamp for the learned MAC address.

Statistics

The Statistics table shows PRP statistics for port A and port B of the selected channel. You can also display historical values for LAN A and LAN B Wrong Count and Network Fault Count in the multiline chart.

- Select the time unit for the chart: **1 Hour** (the default), **1 Day**, or **1 Week**.

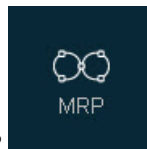
The chart is blank if there is no data for the selected time unit. By default, IND stores data for 7 days, but you can use **Settings > System Settings > Data Collection** to change the metrics data retention period from 1 to 31 days.

- Select or deselect the boxes in the legend to display only the data for the counters you select.
- Hover the mouse pointer over a line to display the numerical values for points on the line.
- Click **View Details** to view the chart in pop-up window where you can select a range for the data.

Port A, Port B	Port connected to LAN-A or LAN-B.
Name	Name of the PRP channel interface.
Network Status	Status of the PRP port: Up (in use) or Down.
Transmit Count	Number of frames sent over port A or port B.
Receive Count	Number of frames received over port A or port B.
Wrong LAN Count	Number of frames with the wrong LAN identifier received on port A or port B.
Unique Entry Count	Number of entries in the duplicate detection mechanism on port A or port B for which no duplicate was received.
Duplicate Entry Count	Number of entries in the duplicate detection mechanism on port A or port B for which one single duplicate was received.

Multiple Entry Count	Number of entries in the duplicate detection mechanism on port A or port B for which more than one duplicate was received.
Network Fault Count	Number of frames with errors received on port A or port B.
LAN Error Count	Number of frames with the wrong LAN identifier received on port A or port B.

MRP



Click the MRP menu tile on the device details page to display information about Media Redundancy Protocol (MRP) on the device. MRP details are available when the MRP feature is supported and configured on a licensed device. Devices must have an MRP licence to use MRP.

Media Redundancy Protocol (MRP) is a data network protocol standardised by the International Electrotechnical Commission as IEC 62439-2. It allows rings of Ethernet switches to overcome any single failure with recovery time much faster than achievable with Spanning Tree Protocol. It is suitable to most Industrial Ethernet applications.

MRP operates at the MAC layer and is commonly used in conjunction with the PROFINET standard for industrial networking in manufacturing.

MRP provides fast convergence in a ring network topology for Industrial Automation networks. MRP Media Redundancy Manager (MRM) defines its maximum recovery times for a ring in the following range: 10 ms, 30 ms, 200 ms, and 500 ms.

The switch supports two modes of MRP; however, only one mode can be enabled to operate on the switch at any given time:

- PROFINET MRP mode—Deployed in a PROFINET environment, the switch is added and managed by Siemens Totally Integrated Automation (TIA) Framework. This is the default MRP mode if the MRP manager or client license is activated through the web interface or command line.
- MRP Command-line interface (CLI) mode—This mode is managed by the Cisco IOS CLI and WebUI, a web-based user interface (UI).



Note For more information about MRP, see [Media Redundancy Protocol Configuration Guide for IE 2000, IE 4000, IE 4010, and IE 5000 Switches](#) or [Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches](#).

MRP information is refreshed every 15 minutes. To change the frequency at which this information is updated, change the data collection timing for metrics status poller under the **Settings > System Settings > Data Collection** page.

If the device is configured for more than one MRP ring, select the MRP ring number for which you want to view statistics from the drop-down menu.

Overview	
Domain Name	A user-defined unique logical name for the MRP ring.
Domain ID	A universally unique identifier (UUID) that identifies the ring.
Network Topology	Ring.
Network Status	Whether the MRP ring is Open or Closed (MRM only).
Configuration Mode	Shows how the node is configured: Auto-Manager, Manager, or Client. Note The MRA role is not an operational MRP role like Manager or Client. It is only an administrative, temporary role at device startup, and a node must transition to the Manager role or the Client role after startup and the Manager is selected through the Manager voting process.
Best Manager MAC Address	(Auto-Manager and non-PLC) MAC address of the node selected as Manager through the Manager voting process.
Best Manager Priority	(Auto-Manager and non-PLC) Configured priority of the node selected as Manager through the Manager voting process.
Operational Mode	Shows the MRP role of the node: Client or Manager
VLAN ID	VLAN for sending MRP frames.
Configured From	Shows whether MRP is configured from CLI or Profinet.
Priority	(Shown when Configuration Mode is Manager) Configured priority value used in the Manager voting process.
License	(Not applicable for Profinet PLC) Shows whether the MRP license is Active or Inactive.

Profile	(Not applicable for Profinet PLC) The recovery time profile, composed of various parameters, which drives the MRP topology convergence performance. The 200 ms profile supports a maximum recovery time of 200 ms. The 500 ms profile supports a maximum recovery time of 500 ms.
Port Details	
Port-1, Port-2	MRP ring ports.
MAC Address	MAC address of the ring port.
Interface	Interface name of the ring port.
Status	The state of the ring port: <ul style="list-style-type: none"> • Disabled—All packets received by the port are dropped. • Blocked—All packets received by the port are dropped, with the exception of MRP protocol packets. • Forwarding—All packets received by the port are forwarded. • Not Connected—The link is physically down or disconnected. (This state differs from the Disabled state, in which the MRP Port is manually disabled through software.)

Licensed Device Details - CIP Device

Details for Licensed CIP devices (EtherNet/IP nodes) include an overview of the device and a table listing information about the device modules. Details also include information about DLR and PTP for CIP devices that support these features.

If the device is in Unlicensed state, the Licensed Device details page displays a link to move the device to Licensed state.

- Click **View Topology** to open the Topology page with the device selected.
- Click **Discover Bridged Devices** to trigger backplane bridged discovery on all communication modules in the device. This button is displayed if the device supports CIP routing.

This option is available on CIP devices that support the Backplane bridging feature. You can view the feature list on the Inventory page.

- Click **Open Device Manager** (available if device is IP Reachable) to open Device Manager in a new tab.
- Click **Refresh CIP Device Data** to perform an on-demand data refresh on the device.

- Click **Update Device** to manually update device details.

You may want to manually update the device information when the CIP device does not return all the information needed during discovery, such as MAC address or Serial Number, or if you want to add custom values for the fields. You cannot modify the Protocol field or the IP Address field of CIP modules but you can modify the chassis IP address.

If you do not specify a value for the Name field, the default is the hostname or IP address returned by the device at discovery. The value for Name is sent as the Asset Name for a device to ISE through pxGrid.



Note Manually updated field values take priority over automatic updates. That is, the manually updated value will not be overwritten with the data fetched from the device during periodic data refresh. After you update an attribute for a device, it will never be updated by automatic discovery until the device is deleted and re-discovered.

Manually updated fields are flagged in the Device Overview with an "Edited" label.

- On DLR-capable devices, click the **DLR** menu tile on the left of the page to display Device Level Ring (DLR) parameters and statistics for a DLR node. For details, see [DLR, on page 53](#).
- Click the PTP menu tile on the left of the page to display Precision Time Protocol information for the device. See [PTP, on page 54](#).
- Click the PRP menu tile on the left of the page to display Parallel Redundancy Protocol (PRP) information for the device. See [PRP, on page 63](#).

Table 11: Device Overview

Name	Name of the CIP backplane device.
Host Name	The device host name.
IP Address	IP address of the device in dot-decimal notation.
MAC Address	MAC address of the device.
Product ID	Product Identifier
Hardware Version	Device hardware version number.
Software Version	Software revision string for the device.
Vendor	Name of the manufacturer of the device.
Description	Description of the device.
IP Reachable	If the CIP device IP address can be pinged by IND and the device was discovered through asset discovery, then this field is not visible on the device details page. If the device cannot be pinged, this field is visible and is set to no.

Protocol	CIP
Device Type	EtherNet/IP node
Group	Concatenation of all names in the unique path from root to the parent of the group, separated by ">".
Serial Number	The device serial number.
Connected to	<p>Names of the devices that this device is connected to.</p> <p>If there are more than four connected devices, the count is shown as a hyperlink. Click on the link to open a pop-up window with the list of devices.</p> <p>Click the connected device name link to display the device details, if that device has been discovered by the system. For Licensed Device ports only, click the port name link to display port details.</p> <p>Note Links are shown only for the devices in your Auth Group and subgroups. For other devices, the links are disabled.</p>
Tag(s)	<p>The tags associated with this device.</p> <ul style="list-style-type: none"> • If tags are associated with this device, the tag names are displayed as a link. Click the link to display the Associated Device Tags pop-up window to add or remove tags. • If no tags are associated with the device, + is displayed as a link. Click the link to display the Associated Device Tags pop-up window to add or remove tags.
pxGrid Asset	Indicates whether the device is considered a pxGrid asset and sent to ISE.

Table 12: Additional Details

Discovered through CIP routing with path	CIP extended path of how this device was discovered. Format: Device1 / Slot-x (IP-y) > Device2 / Slot-x (IP-y) > ...
PLC Program Names	List of names of programs running on the controller modules if this device has controller modules.

Discovered As	<p>The IP address through which this device was discovered. For example:</p> <ul style="list-style-type: none"> • Device behind backplane: Discovered as 192.10.10.85 via Slot-2 (192.10.10.85) • NATed device: Discovered as 10.195.119.50 via Slot-2 (192.10.10.85) • IP reachable device: Discovered as 192.10.10.85 via Slot-2 (192.10.10.85) <p>Where:</p> <ul style="list-style-type: none"> • 192.10.10.85 is module IP address. • 2 is the module slot number. Will be 0 for single slot devices. • 10.195.119.50 is NAT outside IP address.
---------------	--

Table 13: CIP Modules

Slot	Communication module slot number.
Vendor ID	Unique ID number of the device manufacturer.
Product Type	CIP device product type code.
Device Profile	Standard device classification that defines the capabilities and characteristics of this CIP device.
Product Code	Vendor assigned numeric product code identifier.
Revision	Revision number of the CIP device.
Status	CIP device status code, from the CIP Common Specification.
Serial Number	Vendor-specific serial number string for the device.
Product Name	Vendor-specific product name of the CIP device.
IP Address	The IP address that was used to open the CIP connection.
MAC Address	CIP device MAC address.
Subnet Mask	Subnet mask for this CIP device.
Port Name	CIP port name.

Licensed Device Details - PROFINET PLC

Details for Licensed PROFINET Programmable Logic Controller (PLC) devices include an overview of the device and additional details listing protocol-specific information. Details also include MRP information.

If the device is in Unlicensed state, the Licensed Device details page displays a link to move the device to Licensed state.

- Click **View Topology** to open the Topology page with the device selected.
- Click **Retrieve Device Data** to perform an on-demand data refresh on the device.
- Click **Update Device** to manually update device details.

You may want to manually update the device information when the device does not return all the information needed during discovery, such as MAC address or Serial Number, or if you want to add custom values for the fields. You cannot modify the Protocol field or the IP Address field.

If you do not specify a value for the Name field, the default is the hostname or IP address returned by the device at discovery. The value for Name is sent as the Asset Name for a device to ISE through pxGrid.



Note Manually updated field values take priority over automatic updates. That is, the manually updated value will not be overwritten with the data fetched from the device during periodic data refresh. After you update an attribute for a device, it will never be updated by automatic discovery until the device is deleted and re-discovered.

Manually updated fields are flagged in the Device Overview with an "Edited" label.

- On MRP-capable devices, click the **MRP** menu tile on the left of the page to display Media Redundancy Protocol (MRP) parameters and statistics for a MRP node. For details, see [MRP, on page 67](#).

Table 14: Device Overview

Name	Name of the device.
Host Name	The device host name.
IP Address	IP address of the device in dot-decimal notation.
MAC Address	MAC address of the device.
Product ID	Product Identifier
Hardware Version	Device hardware version number.
Software Version	Software revision string for the device.
Vendor	Name of the manufacturer of the device.
Description	Description of the device.
Protocol	PROFINET

Device Type	Controller
Serial Number	The device serial number.
Group	Concatenation of all names in the unique path from root to the parent of the group, separated by ">".
Connected to	<p>Names of the devices that this device is connected to.</p> <p>If there are more than four connected devices, the count is shown as a hyperlink. Click on the link to open a pop-up window with the list of devices.</p> <p>Click the connected device name link to display the device details, if that device has been discovered by the system. For Licensed Device ports only, click the port name link to display port details.</p> <p>Note Links are shown only for the devices in your Auth Group and subgroups. For other devices, the links are disabled.</p>
Tag(s)	<p>The tags associated with this device.</p> <ul style="list-style-type: none"> • If tags are associated with this device, the tag names are displayed as a link. Click the link to display the Associated Device Tags pop-up window to add or remove tags. • If no tags are associated with the device, + is displayed as a link. Click the link to display the Associated Device Tags pop-up window to add or remove tags.
pxGrid Asset	Indicates whether the device is considered a pxGrid asset and sent to ISE.

Table 15: Additional Details

Role	Role of the device in the PROFINET IO system.
Annotation	Manufacturer specific annotation string for the device.

Other Device Details

Device details for devices other than Licensed devices (for example, HMI devices) include an overview and additional details about the device.

- Click **View Topology** to open the Topology page with the device selected.
- Click **Update Device** to manually update device details.

You may want to manually update the device information when the device does not return all the information needed during discovery, such as MAC address or Serial Number, or if you want to add custom values for the fields. You cannot modify the Protocol or the IP Address fields.

If you do not specify a value for the Name field, the default is the hostname or IP address returned by the device at discovery. The value for Name is sent as the Asset Name for a device to ISE through pxGrid.



Note Manually updated field values take priority over periodic updates. That is, the manually updated value will not be overwritten with the data fetched from the device during periodic data refresh. After you update an attribute for a device, it will never be updated by periodic data refresh.

Manually updated fields are flagged in the Device Overview with an "Edited" label.

- Device Overview
 - Displays Name, Host Name, IP Address, MAC Address, Product ID, Hardware Version, Software Version, Vendor, Description, Protocol, Device Type, Serial Number, Group, Connected Device, associated device tags, and whether the device is a PxGrid Asset.

Protocol is shown as UNKNOWN for unknown protocol devices. Attributes such as Product ID show Unknown or NA if the information cannot be obtained during discovery or has not been updated manually.
 - For manually added devices, Added By and Added Time attributes are also displayed.
- Additional Details—displays protocol-specific information and details on modules, depending on the industrial protocol and device type.

For BACnet/IP, CIP, MODBUS, PROFINET, and OPC UA devices, the system assigns device type during discovery. You can manually set the device type by clicking **Update Device** to select a device type from the drop-down menu or enter a custom device type name if required.

Port Details

Port details are available for Licenced IE switches in the Licensed state and include port description, status, settings, bandwidth chart, and port metrics. You can access port details in the following ways:

- Click the link in the Connected To column on the Inventory page, then click the port name in the Connected Devices pop-up window.
- Click on a port name link on the Connected Devices page of Device Details.
- Click on a link in the Topology map to display the connected devices and ports, then click a port name link.
- On the Device details page for the switch, in the physical device view section, click on the port on the faceplate and then click the port name link in the pop-up window.

On the port details page, you can perform these actions:

- Click **Open Device Manager** to launch the Device Manager application on the device. You must have a Device Manager user name and password.
- Click the links under Connected Devices to see details for the device or port that this port is connected to.
- The Bandwidth chart shows bandwidth utilization on the port. Click **1 Hour**, **1 Day** or **1 Week** to select the time scale of the chart. Click the blue or red box to select the type of utilization to display (Rx or Tx). Click **View Details** to view the chart in a pop-up window and select a specific time period.

Device Prerequisite Configuration

The following information describes the CLI configuration required for the system to discover a Licensed device and transition the device from Unlicensed to Licensed state. This section also describes the Device Manager configuration required on IE 1000 switches.



Note A local account is not needed on the device if TACACS is available.

Configuration Required for Discovery and Management of IOS Devices

Follow these steps to configure the switch so that IND can discover the device and transition it from UNLICENSED to LICENSED state.

1. Enter global configuration mode:


```
configure terminal
```
2. Configure SNMP to allow the system to successfully discover the device:


```
snmp-server community read-community ro
```

read-community must match the SNMP V2 Read string defined in the system Access Profile that is attached to the Discovery Profile. The default read community string is "public".
3. Enter the following command to allow the system to discover a Licensed device and transition the device from UNLICENSED to LICENSED state with SNMPv3. The group that you create and the mode are used to associate with the SNMPv3 user that you configure in the next step. Based on the mode that you choose for the group, you can configure the authentication, privacy protocols and passwords for the user.

```
snmp-server group group_name v3 mode
```

where *mode* is one of the following:

- **priv**: Enables Data Encryption Standard (DES) packet encryption.
- **auth**: Enables the Message Digest 5 (MD5) and the Secure Hash Algorithm (SHA) packet authentication.
- **noauth**: Enables the noAuthNoPriv security level. This is the default if no keyword is specified.

4. Add a new user for the SNMP group:

```
snmp-server user user_name group_name v3 [auth authentication_type authentication_password [priv privacy_type privacy_password]]
```

- **auth**: Specifies an authentication level setting session that can be either the HMAC-MD5-96 (**md5**) or the HMAC-SHA-96 (**sha**) authentication level and requires a password string *auth-password* (not to exceed 64 characters).
 - **priv**: Configure a private (**priv**) encryption algorithm and password string *privacy-password* (not to exceed 64 characters). Supported *privacy_type* values are: **aes**, **128**, and **des**.
5. Configure the following for the system to successfully transition the device from UNLICENSED to LICENSED state. This should match the device access username and password specified in the system Access Profile.


```
username username privilege 15 password 0 password
```
 6. Enter the following commands to configure authentication, authorization, accounting (AAA):


```
aaa new-model
aaa authentication login default local
aaa authorization exec default local
```
 7. Configure the Secure Shell (SSH) server:


```
ip ssh version 2
```
 8. Configure the HTTP/HTTPS server:


```
ip http server
ip http secure-server
ip http authentication aaa login-authentication default
```
 9. Configure the number of Telnet sessions (lines) and a Telnet password for the line or lines:


```
line vty 0 15
login authentication default
transport input all
transport output all
```
 10. Return to privileged EXEC mode:


```
end
```

Device Manager Configuration Required for Discovery and Management of IE 1000 Switches

1. Log in to the IE 1000 Device Manager.
2. Leave the username field blank and enter **cisco** as password.
3. Choose **Admin > Users**.
4. Create Device Access User and use the same in Access Profile on the system.
5. Configure SNMP community string for Read Only (ro):
 - a. Choose **Configure > SNMP**. Click **OK** in the pop-up window to confirm enabling SNMP.
 - b. Check the check box to enable SNMP Mode globally. Click **Submit**.
6. Select Community Strings tab. Add a *public* Community String with read only access. (By default, this is a Read Only (ro) string).

For SNMPv3:

- a. Select the Users tab and add an snmpv3 user with name, security level, authentication protocol, authentication password, privacy protocol, and privacy password. Click Ok.
- b. Select the Group tab, select the created user, and specify the group name. Click Ok.

7. Choose Admin > Access Management.

- a. Check the check box to enable SSH or Telnet. (This option determines how the IE 1000 communicates with the system).
- b. Click **Submit**.

Configuration Required for Topology Discovery of SNMP Devices with SNMPV3

All SNMPV3 devices that are not managed by IND should have prerequisite configuration for the SNMP context, which is required to query the BRIDGE-MIB with SNMPV3 security. A sample configuration for IOS devices is given below.

```
#Device prerequisite configuration for device discovery of IOS devices with SNMPV3 security
#Supported mode values are [priv, auth, noauth]
snmp-server group {group_name} v3 {mode}

#Supported authentication_type values are [sha, md5]
#Supported privacy_type values are [aes 128, des]
# The group created with mode will be used by the below CLI command for associating the
SNMPV3 user with that mode.
#According to the mode chosen, user can configure the authentication, privacy protocol and
passwords.
snmp-server user {user_name} {group_name} v3 [auth {authentication_type}
{authentication_password} [priv {privacy_type} {privacy_password}]]

#The system needs the following additional configuration to be able to query bridge-mib
with SNMPV3 security in IOS devices.
#This bridge-mib is required to get MAC-Table from SNMP for topology discovery.
snmp-server group {group_name} v3 {snmpv3_mode} context vlan- match prefix
```

Bootstrap Configuration

The system pushes the following configuration when you move the device to the Licensed state in the system:

```
# Secure-mode only
# Only if user selected self-signed certificate for device certificate in access profile
# If the device has a self-signed certificate with RSA key pair length < certificate key
length given in access profile (or) if the device does not have a self-signed certificate
in nvram

crypto key generate rsa label IND_HTTPS_CERT_KEYPAIR modulus {certificate-key-length}
crypto pki trustpoint IND_HTTPS_CERT_KEYPAIR
enrollment selfsigned
subject-name OUT="IOT"
rsa-keypair IND_HTTPS_CERT_KEYPAIR
hash sha256
crypto pki enroll IND_HTTPS_CERT_KEYPAIR
# Enable SCP server
# Used for transferring ODM file from the system to device
# For insecure mode the system uses FTP to transfer ODM file
ip scp server enable

# If AAA is not enabled on the device
```

```
ip http authentication local
#Secure mode only
ip http secure-server
ip http secure-port {secure-mode-access-port}
#Insecure mode only
ip http server
ip http port {regular-mode-access-port}

# Configure WSMA
# The system uses WSMA for management
wsma agent exec
profile exec
# Secure-mode only
wsma profile listener exec
transport https path /wsma/exec
# Insecure mode only
wsma profile listener exec
transport http path /wsma/exec

# SNMP configuration
# Trap destination. The system supports both v2c and v3
snmp-server host <system-ip-address> version 2c {snmpv2-read-community} udp-port 30162
# Trap destination for v3 security
snmp-server host {system-ip-address} version 3 {snmpv3_mode} {snmpv3_username} udp-port 30162

# Bootstrap configuration for SNMPv3
# The system needs the following configuration to be able to query bridge-mib with SNMPv3
security in IOS devices.
# This bridge-mib is required by inventory service to get MAC-Table from SNMP when the
system moves device from new to managed state.
snmp-server group {group_name} v3 {snmpv3_mode} context vlan- match prefix
# Enable RFC2233 compliant for linkDown and linkUp trap
snmp-server trap link ietf

# Enable traps supported by the system
snmp-server enable traps snmp linkdown linkup coldstart
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps rep
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
snmp-server enable traps flash insertion removal
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps alarms informational
snmp-server enable traps errdisable
snmp-server enable traps mac-notification change move threshold

# Configure SNMP to retain ifindex across reboots
snmp ifmib ifindex persist

# Enable dual-power supply
# Not applicable for S5410, IE5K, CGS2K, IE3010
power-supply dual

# Enable SD card alarm
# Not applicable for S8000, CGS2K, IE2000U, IE3010, IE3K, IE3200, IE3300, IE3400 and S5800

alarm facility sd-card enable
alarm facility sd-card notifies
```

```
# Turn on notifies for selected facility alarms
alarm facility temperature primary notifies
alarm facility temperature secondary notifies
# Following not application for CGS2K, IE3010
alarm facility power-supply notifies
no alarm facility power-supply disable
```

Bootstrap Configuration for IE 1000 Switches

```
# Traps for IE 1000
snmp.config.trap_source.add coldStart
snmp.config.trap_source.add warmStart
snmp.config.trap_source.add linkDown
snmp.config.trap_source.add linkUp
snmp.config.trap_source.add topologyChange
snmp.config.trap_source.add authenticationFailure
snmp.config.trap_source.add entConfigChange
snmp.config.trap_source.add fallingAlarm
snmp.config.trap_source.add risingAlarm
snmp.config.trap_source.add newRoot

# Trap destination
snmp.config.trap_receiver.add <system-ip-address> version 2c {snmpv2-read-community} udp-port
 30162

# Trap destination for v3 security
snmp.config.trap_receiver.add {system-ip-address} version 3 {snmpv3_mode} {snmpv3_username}
  udp-port 30162
```

Topology

Operate > **Topology** displays a network topology map of devices based on groups. The Root group is displayed by default when you first view the topology. You can select groups and subgroups to display in the topology as described below. The types of devices that the system displays in the topology map, represented by various icons, include Industrial Ethernet (IE) switches and other devices that run automation protocols. You can display a legend of the device icons (described in the Layout section below).

When IND discovers devices through Link Layer or IP Scan discovery (see [Discovery, on page 24](#)), it automatically initiates a topology discovery for the set of discovered devices. Topology discovery is also automatically initiated when a LINK UP trap is received for a device connected to the port of a discovered Licensed device in the Licensed state. You can view information about topology discovery tasks in the [Tasks, on page 125](#) and [Audit Trails, on page 22](#) pages.

Links in the topology are represented by straight lines that connect the device icons in the map. If you hover the mouse over a straight line, a pop-up label appears that shows the actual number of links between the device and connected devices.

When SNMP is enabled on the devices and used in the access profile for discovery, IND will also use MAC address table and ARP (Address Resolution Protocol) table entries on the devices to discover other neighbour devices in the network in addition to LLDP (Link Layer Discovery Protocol) and CDP (Cisco Discovery Protocol). LLDP and CDP discovered links take precedence over the links discovered through MAC address table and ARP table entries.



Note The links to connected devices discovered only through MAC address table and ARP entries may not always represent physical connections.



Note If a link between two switches that was previously discovered is found to be operationally down in the next topology discovery run, the unreachable device or link is displayed in the topology with an alarm indication, if the operational down alarm exists. The topology is updated after the device becomes reachable or any link up alarms are received (resulting in the closure of the previous alarm).

The system also displays links between a switch, Virtual Machines (VMs), and VMware ESXi server.

- When SNMP is enabled on the ESXi server, the links are shown from the server to the VMs on it.
- When SNMP is not enabled on the ESXi server, links are shown from the switch connected to the ESXi server to the VMs on the ESXi server along with other neighbors.

The CIP interface name shown on links involving CIP devices does not always represent the physical interface name on the device.

You can display an overlay of VLANs, DLR networks, PTP, and REP configured on devices within a group (described below).

Display Group Information

The group hierarchy is displayed in the left pane, with the number of devices in the group displayed next to the group name. The group hierarchy displayed is based on the Context Group drop-down menu selection. The Context Group drop-down menu lists the groups and subgroups that you can access based on your group assignment. See [Buttons and Controls, on page 123](#) for information about the Context Group menu.

To display group information:

- Click a group name in the navigation pane on the left of the page to display the group's assets and subgroups in the map area on the right. Click **Find Groups** to enter text to filter or search for groups by name.

The topology map displays the topology for the selected group and subgroups. Devices that are members of the group are shown as icons that represent the device type, along with a label that shows the device name. Connected devices that are not part of the group are included in the topology but appear grayed out.

- Groups are labeled in the topology map with the group's name. For groups with a large number of devices, you may need to use the zoom function (described below) to see the label. Hover over or click the group name to highlight the members of the group.

Modify and Save Layout

There are several ways you can modify the layout of the topology map and save your changes:

- Drag and drop icons in the topology to modify the layout.
- Use the controls on the bottom right of the map area to toggle full screen, zoom in or out, and display a legend.
- Use the menu on the upper left of the map area to access these functions:
 - **Layer:** Select VLAN, DLR, PTP, or REP to view details about these features for the group. See [VLAN Layer, on page 83](#), [DLR Layer, on page 83](#), [PTP Layer, on page 84](#), and [REP Layer, on page 85](#).

- **Refresh:** Click to refresh the map after a topology discovery.
- **Save:** Click to save the layout. Your layout is saved for the next time you access the Topology page.
- **Discover Topology:** Click to manually trigger a discovery of the topology. Neighbor discovery is initiated for all the nodes in the selected group and its subgroups. Refresh the topology page after the task is complete to see the latest information. The updated topology map displays links between devices and changes in the topology of a group, such as devices that are added or removed.

If a topology discovery task is already running for the selected group, the system displays a message to inform you of the existing task and asks if you want to initiate another. Click **No** to keep the current task. Click **Yes** to initiate a new topology discovery.



Note

- When the physical topology of devices is modified, device refresh and manual Discover Topology update connected devices and topology links in IND.
- Topology discovery occurs only when you invoke manual Discover Topology for existing devices in IND or when devices are rediscovered in IND. Metric or inventory collection does not cause topology discovery.
- Discover Topology updates the connected devices information; device refresh does not.
- Occasionally, when multiple IP scan discoveries are triggered in parallel, the topology discovery might not always be in sync with the device discovery. This might result in links not properly shown between devices discovered through different IP scan discoveries. In such cases, it is necessary to manually trigger Discover Topology after all the IP scan discoveries are completed for links between the devices to be properly shown.
- The Topology page and the Connected Devices tab are updated only with device rediscovery and Discover Topology. If a redundancy protocol is configured on discovered and licensed devices, the Topology page and the Connected Devices tab are not automatically updated. You must delete and rediscover the devices and manually invoke Discover Topology.

To save a screen capture of the topology in PNG format, click the upload button on the right of the device search box on the upper right of the Topology page.

Display Device and Link Information

To display device information:

- To view a summary of device-specific details, click on the device icon in the topology map to view the details in a pop-up panel on the right of the map area. Click the device name link to go the Device Details page for the device. (See [Device Details, on page 48](#).)

You can enter a device name, IP address, or device type in the search box on the upper right of the Topology page to highlight the device on the map and display the details.

- If alarms exist for a device, an alarm icon is displayed next to the device in the topology map. To view details about device alarms, click the **Alarms** link in the pop-up to view the alarm details on the **Operate > Alarms** page.
- To view details about a link, click on the link and then click the device name in the pop-up link summary. (See [Port Details, on page 75](#) for information about the Port Details page.)

Moving and Tagging Devices

To select devices in the topology map and move the devices to a different group or tag the devices:

- Select a device by clicking on it in the topology map. Hold the Shift key to select multiple devices.
- To move the selected device(s) to a different group, click **Actions > Move to Group** in the pop-up panel on the right, select a group in the Move Selected Device(s) drop-down list, and confirm the move when prompted.
- To associate tags with the selected device(s) or remove associated tags, click **Actions > Tags** in the pop-up panel on the right, select **Security** or **Regular**, select the tags in the drop-down list, click **Add** or **Remove**, and confirm the action when prompted.

See [Tags, on page 115](#) for more information.

VLAN Layer

You can view VLANs on the topology map.

The VLANs available for display are all the VLANs collected for all switches in the Licensed state in the group. If the group does not contain any switches or if the switches are not in the Licensed state, there are no VLANs to display. For a VLAN link to be displayed, both nodes must have the VLAN defined and assigned to the physical port of the link.

To display VLANs configured on devices within a group, click **Layer** at the top left of the topology map, and then select a VLAN ID from the drop-down list.

- The devices in the selected VLAN and links are highlighted.
- Click a device in the VLAN to display VLAN information, including VLAN name and member ports, in the pop-up panel on the right.
- Click the device name link in the pop-up panel to go the Device Details page for the device. (See [Device Details, on page 48](#).)
- Click **Reset** in the **Layer** pop-up to remove the VLAN layer from the map.

DLR Layer

A Device Level Ring (DLR) network is a single-fault tolerant ring network used to connect automation devices. You can view a DLR network on the topology map when the DLR ring supervisor is licensed. The supervisor must be licensed because the ring member information is obtained only from a supervisor. Any device that supports DLR can be licensed.

A DLR network has the following elements:

- **Ring Node:** A ring node is any node that operates on the network to process data that is transmitted over the network or to pass on the data to the next node on the network. When a fault occurs on the DLR network, ring nodes reconfigure themselves and relearn the network topology.
- **Active Supervisor:** A ring supervisor blocks most traffic on one of its ports to prevent packets circulating forever in the ring. It also sends Beacon frames or Announce frames. When multiple nodes are enabled as supervisor, the node with the numerically highest precedence value becomes the active ring supervisor; the other nodes automatically become back-up supervisors.

- **Backup Supervisor:** During normal operation, a back-up supervisor behaves like a ring node. If the active supervisor node operation is interrupted, the back-up supervisor with the next numerically highest precedence value becomes the active supervisor.
- **(Optional) Active Redundant Gateway and Backup Redundant Gateway:** Allows a device on the DLR network to connect to the outside network.

To display DLR configured on devices within a group, click **Layer** at the top left of the topology map, and then select **DLR**. Select a DLR ring from the drop-down list or select **See All Supervisors**.

- The devices in the selected DLR ring and links are highlighted and Active and Backup Supervisors for the ring are labeled.
- Click a DLR link to display the DLR link status. A dotted line represents a blocked port on the Active Supervisor.
- The interface information on the links between switches and non-switches is not available if the ports participating in the selected DLR ring are down.
- Click a DLR device in the ring to display information about DLR status, roles, and ports in the pop-up panel on the right.
- Click the device name link in the pop-up panel to go the Device Details page for the device, and then click the **DLR** menu tile to view the DLR parameters and statistics for the DLR node. (See [DLR](#), on page 53.)
- Click **Reset** in the **Layer** pop-up to remove the DLR layer from the map.

PTP Layer

Precision Time Protocol (PTP) synchronizes with nanosecond accuracy the real-time clocks of the devices in a network. Using the best master clock selection, a device identifies the port that is connected to a device with the best clock source. The device then synchronizes its internal clock with that clock source. The most precise clock source in the network is referred to as the grandmaster clock.

To display PTP configured on devices within a group, click **Layer** at the top left of the topology map, and then select **PTP**. Select a PTP device from the drop-down list or select **See All Grandmaster Clocks**.

- The devices in the selected PTP network are highlighted and are labeled according to their clock type:
 - GM: Grandmaster
 - S: Slave
 - TC: Transparent clock
 - BC: Boundary clock
- Yellow curved lines show devices in the group that synchronize to the grandmaster.
- Click a PTP device in the network to display PTP status. For descriptions, see [PTP](#), on page 54.

You can also click the device name link in the pop-up panel to go the Device Details page for the device, and then click the **PTP** menu tile to view the PTP information for the device.
- Click **Reset** in the **Layer** pop-up to remove the PTP layer from the map.

REP Layer

Resilient Ethernet Protocol (REP) provides an alternative to Spanning Tree Protocol (STP) to control network loops, handle link failures, and improve convergence time. REP is a segment protocol and is supported on Layer 2 trunk interfaces only.

Each end of a segment terminates on an edge switch. Each segment on a switch must have a unique segment ID. The port where the segment terminates is called the edge port. Each segment consists of standard (non-edge) segment ports and up to two edge ports. A device can have only two ports that belong to the same segment, and each segment port can have only one external neighbor. REP guarantees that there is no connectivity between two edge ports on a segment.

One edge port in a REP segment acts as the primary edge port; the other as the secondary edge port. It is the primary edge port that always participates in VLAN load balancing in a REP segment. REP VLAN load balancing is achieved by blocking some VLANs at a configured alternate port and all other VLANs at an edge port. The execution (preemption) of VLAN load balancing is triggered by manually enforcing it or after a pre-defined delay, after the REP segment is complete. When the segment is completed, all ports are in the open (forwarding) state except the alternate port used for VLAN load balancing:

- When all interfaces in the segment are UP, the alternate port is blocking.
- When a link or switch failure occurs on the segment, the blocked port begins forwarding.

To display REP configured on devices within a group, click **Layer** at the top left of the topology map, and then select **REP**. Use the drop-down list to select a REP segment and click **Apply**. REP segments are shown in the format *EdgeNode:segment number* (Primary/Secondary). When a segment is complete, the drop-down menu shows *PrimaryEdgeNode:segment* (Primary). If there is a failure, the menu shows *SecondaryEdgeNode:segment* (Secondary).

- REP segment nodes and links are highlighted. Segment nodes are labeled as Primary Edge, Primary Edge No-Neighbor, Secondary Edge, Secondary Edge No-Neighbor, and Alternate.
- Click a REP link to display the REP link status. A dotted line represents a blocked port or a blocked VLAN on a primary edge port.
- Click on a node in the segment to display a summary of the device and REP information in the pop-up panel on the right.
- Click the device name link in the pop-up panel to go the Device Details page for the device, and then click the **REP** menu tile to view detailed REP information. (See [REP](#), on page 59.)
- Click **Reset** in the **Layer** pop-up to remove the REP layer from the map.

PRP Layer

To display Parallel Redundancy Protocol (PRP) configured on devices within a group, click **Layer** at the top left of the topology map and select **PRP**. Select **Show PRP Node Details** or **Show PRP Node Connections** from the drop-down list. If you select **Show PRP Node Details**, optionally select VLAN IDs that are part of the PRP network from the **Select VLAN** drop-down list to see an overlay of the VLANs in the PRP topology. Click **Apply**.

- Show PRP Node Details—PRP nodes are highlighted with a dark background. Click a PRP node to display a summary of the device and PRP information in the pop-up panel on the right. PRP node details can be displayed only for Redbox and DAN, not for VDAN and LAN devices.



Note See [PRP](#), on page 63 for PRP field descriptions.

When you select a VLAN ID, all the nodes that are part of the VLAN are highlighted in a different color. Note that the VLAN overlay also highlights nodes and links to other neighbors that are not part of the PRP network topology.

- Show PRP Node Connections—PRP nodes are highlighted with a dark background. Click a PRP node to display the members of the same PRP topology, indicated by a yellow line.

The devices in the selected PRP network are labeled as follows:

- Redbox—Redundancy Box
- DAN—Dually Attached Node
- VDAN—Virtual DAN
- SAN-A—Singly-Attached Node connected to LAN-A
- SAN-B—Singly-Attached Node connected to LAN-B
- LAN-A—Infrastructure switches that are connected to LAN-A and not configured as RedBox.
- LAN-B—Infrastructure switches that are connected to LAN-B and not configured as RedBox.



Note For devices to be labelled properly in the topology page, all REDBOX nodes that are part of the PRP channel must be discovered and licensed.

Devices that are part of the PRP network are labelled as SAN-A or SAN-B if they are discovered in the PRP network and found to be non-switch devices. Otherwise, SAN devices are labelled as LAN-A or LAN-B.

LAN-A or LAN-B labels indicate the PRP node status as follows:

- Green border—OK
- Red border—BAD

The status shown applies to all the nodes that are part of the PRP network. Because a node can participate in multiple PRP channels at the same time, the status is **OK** only if there are no interfaces down in all the PRP channels that the node is part of. If the interface participating in a channel group is down on the REDBOX or DAN nodes, the status of all the LAN nodes that are seen on the network connected to that interface is set to **BAD**.

MRP Layer

To display Media Redundancy Protocol (MRP) configured on devices within a group, click **Layer** at the top left of the topology map, select **MRP**, select the MRP Manager name and ring ID from the drop-down list, and click **Apply**.

- MRP ring nodes are highlighted with a dark background. Click on a MRP ring node to display a summary of the device and MRP information in the pop-up panel on the right.



Note See [MRP, on page 67](#) for MRP field descriptions.

- A solid line represents a link in forwarding mode, and a dotted line represents a link in blocked mode. A dotted red line represents a link that is down.

MRP devices are labeled as follows:

- Manager
- Auto-Manager
- Client



CHAPTER 4

Maintain

- [Cisco Active Advisor, on page 89](#)
- [Configuration Archives, on page 90](#)
- [Software Images, on page 93](#)

Cisco Active Advisor

Cisco Active Advisor is a free cloud-based service that simplifies network discovery and finds security alerts that apply to your devices. It also analyzes contract coverage and end-of-life status. For more information, see [Cisco Active Advisor](#).

When you first log in to the IND system, if you have not already activated Cisco Active Advisor, IND displays a message. Click **Not Now** to continue to **Operate > Dashboard**.

Click **Learn More** to go to **Maintain > Cisco Active Advisor** where you can activate and access the service.

You must have a Cisco Connection Online (CCO) user account to use this service. If you do not have a CCO account, click the **Register Now** link to go to the Cisco.com Registration website and register.

Activate Cisco Active Advisor	Check the check box to use this service.
Last Uploaded Time	If Cisco Active Advisor has been activated, indicates the last time that IND performed a data transfer from devices to Cisco Active Advisor. There is an initial data transfer at activation, after which IND transfers device data monthly (at the end of the month).
CCO User Name	(Displayed when you check the Activate check box) Your Cisco Connection Online user name.
CCO Password	(Displayed when you check the Activate check box) Your Cisco Connection Online password. Reenter this password in the Confirm Password field.

Configuration Archives

Use the Maintain > Configuration Archives page to back up the startup configuration of a device and restore it back to the device as required. You can back up the configuration of all devices periodically based on the configured schedule, or you can back up selected devices on demand. Devices to be backed up must be Industrial Ethernet (IE) switches in the Licensed state, and you must have Configuration Management administrative rights. (System Administrator and Network Administrator roles inherit this permission by default.)



Note You can also display Configuration Archives and perform backup and restore operations by clicking the Device Name to display the Device Details page, and then clicking the **Configuration Archives** tile on the left of the page.

For information about restoring a configuration backup to a device, see [Restore Configuration, on page 92](#).

The Configuration Archives page shows the list of devices and available backups. The link in the Latest Backup column shows the time of the most recent backup. The first backup for a device is designated as Base Version by default. If more than one backup exists, you can choose which file to designate as Base Version (one per device). There can be up to five backups for a device. When the maximum number of backups is reached, the oldest configuration (excluding the Base Version) is rolled over to make room for new configuration backups.

For scheduled backups, the system polls all devices in the Licensed state at the configured interval. The system performs scheduled and on-demand backups as follows:

- If a previous backup for the device does not exist, a backup is performed.
- If a previous backup exists, a new backup is performed only if there is a difference in the configuration from the last backup.

To configure or perform backups:

- To schedule a backup, click the **Schedule** menu tile on the left of the Configuration Archives page. On the Configuration Archives Schedule page, click **Schedule** and select whether to perform the backup weekly or daily, the day of the week for weekly backup, the time of day for the backup, and then click **Save**.

Click **Remove** to remove a scheduled backup.

- To perform an on-demand backup, click the link in the Backup Count column, and then click **Backup Now** in the Configuration Archives pop-up window.
- To view backup file contents, click the timestamp in the Latest Backup column of the main Configuration Archives window for the latest backup or in the Configuration Archives pop-up window for the selected backup.

To view the contents of a previous backup, click the link under Backup Count and click on the link under the backup time. Sensitive information such as passwords is hidden by default. You can choose to display

sensitive information by clicking



- Check the **Base Version** check box (available if there is more than one backup) to designate a backup as the Base Version.
- To delete a backup, click the link under Backup Count, select the backup in the Configuration Archives pop-up window, and click **Delete**.




Note The Base Version cannot be deleted.

- To compare two backup configurations, click the link under Backup Count, select two backups in the Configuration Archives pop-up window, click **With Selected**, and click **Configuration Diff**.

In the Configuration Diff pop-up window, you can choose to view the diff only or the full configuration file. The two configurations are displayed side by side with additions highlighted in green, updates in yellow-orange, and deletions in red. Sensitive information such as passwords is hidden by default. You

can choose to display sensitive information by clicking



Name	Textual description of the device.
Latest Backup	Timestamp of the most recent device configuration backup.  indicates that this is the Base Version.
IP Address	Internet address of the device in dot-decimal notation.
State	Administrative state of the device: <ul style="list-style-type: none"> • Licensed—The system actively manages devices that are in Licensed state. Devices in Licensed state consume a device management license. • Unlicensed—This state refers to devices that can be licensed but have not been moved to Licensed state. The system does not manage devices that are in Unlicensed state. Devices in Unlicensed state do not consume a device management license.
Product ID	Asset tracking identifier of the device.
Software Version	Software revision string for the device.
Group	Concatenation of all names in the unique path from root to the parent of the group, separated by ">".
Backup Count	The number of backups for the device.

Last Backup Run Time	Timestamp of when the backup task was last run on the device. Note This timestamp may be later than Latest Backup because a backup file is created only if there are configuration changes.
Tags	The tags associated with this device. <ul style="list-style-type: none"> • If tags are associated with this device, the tag names are displayed as a link. Click the link to display the Associated Device Tags pop-up window to add or remove tags. • If no tags are associated with the device, + is displayed as a link. Click the link to display the Associated Device Tags pop-up window to add or remove tags.

Restore Configuration

After you back up the current device configuration, you can restore the selected configuration archive to the device. See [Configuration Archives, on page 90](#) for information about configuration archives and backing up the device configuration.

You can restore the configuration only for Industrial Ethernet (IE) switches in the Licensed state. A configuration archive can be restored only for the same device, but the device does not need to be at the same software version. If the device version is lower than the backup version, then some configuration may fail because support would not be available. You must have Configuration Management administrative rights to restore configuration. (System Administrator and Network Administrator roles inherit this permission by default.)

As part of the restore operation, the running configuration is saved to the startup configuration on the device and a backup is created if there is a difference with the last backup. You can view the selected configuration before restoring it. You can also compare the selected configuration to the running configuration.

For IOS devices, the restore is performed on the startup configuration and a device reload is performed. For IE 1000, the restore is performed on the running configuration, and after a successful restore the running configuration is saved to the startup configuration.

To restore a configuration archive:

1. On the Configuration Archives page, select the table row of one or more devices for which you want to restore the configuration and click **With Selected**.
2. Click **Restore** in the pop-up window.
The Restore Configuration window lists the selected devices. The system creates a separate subtask for each device for a restore on multiple devices and these tasks run in parallel.
3. In the Restore Configuration window, select the backup to use for the restore: the latest backup or the Base Version, and then click **Next**.
4. Select whether to review the selected configuration or view the differences between the selected configuration and running configuration.

The two configurations are displayed side by side with additions highlighted in green, updates in yellow-orange, and deletions in red.

5. Click **Restore**.

A task is created to back up the current running configuration of the device and restore the selected configuration archive to the device running configuration.

Software Images


Use the **Maintain > Software Images** page to upload software images that you can use to install device images on demand or associate with a PnP profile. PnP sends the image specified in the profile to a device based on the device type. You can associate up to three images (one per device type) for each PnP profile. See [Plug and Play, on page 5](#) for more information about PnP.

- Click **Upload** to add a software image to the system. Enter a name for the image, and click **Browse** to select an image file to upload.
- To delete an image, select it from the list in the table, click **With Selected**, and then click **Delete** in the pop-up window.



Note If on demand image installation is triggered for more than 6 devices simultaneously, the upgrade occurs in batches of 6 at a time to ensure that server resources are not overloaded.

Name	Name that you assign to the image to be uploaded to the system.
File Name	The image file name; for example, ie2000-universalk9-tar.152-4.EA5.tar. Software images can be in either BIN or TAR file formats.
File Type	The image file format, bin or tar.
File Size (bytes)	The size of the image file.

Version	<p>Software version number of the image.</p> <p>To perform an on-demand installation of the software image on selected devices:</p> <ol style="list-style-type: none"> 1. Click  for the image file that you want to use for the installation. The system displays a list of devices eligible for the installation. 2. Use the Group and Tag(s) drop-down lists to filter devices as needed. 3. Click Next to display the list of filtered devices. You can deselect any of the listed devices on this page. 4. Click Install to begin the installation. <p>Note You can also install the software image for a device on the Operate > Inventory > Device Details page of licensed switches. See Licensed Device Details - Switch, on page 48.</p>
Product Family	Device type that the image applies to.
Date Created	Time when the image was added to the system.



CHAPTER 5

Settings

- [Alarm Settings](#), on page 95
- [Backup](#), on page 100
- [Certificate Management](#), on page 101
- [Device Pack](#), on page 103
- [Group Management](#), on page 103
- [Licenses](#), on page 105
- [Policy Servers](#), on page 108
- [pxGrid](#), on page 109
- [System Settings](#), on page 112
- [Tags](#), on page 115
- [Users](#), on page 116

Alarm Settings

The **Settings > Alarm Settings** page shows the categories of alarms available on the system and the number of alarms in each category. All alarms on the system are enabled by default and have a default severity. You can disable alarms or change the severity to suit your needs. Click on a category to show the alarms in the category.

- To change alarm settings, select the alarms in the list and then click **With Selected**. In the With Selected Alarm Settings pop-up window:
 - Click **Restore** to return the selected alarms to the default settings.
 - To disable or reenable alarms, select **Disabled** or **Enabled** from the Select a Status drop-down list.
 - To change the severity for the selected alarm(s), select a severity from the drop-down list.

Name	Alarm name. See table below for alarm names and descriptions.
Status	The status of the alarm: Enabled or Disabled.
Severity	Alarm severity: Minor, Major, or Critical.

Alarm Name	Description
Device Health	
CPU Utilization High	CPU utilization on the device exceeds the threshold.
Dual Power Supply Failed	The switch monitors dual power supply levels. If there are two power supplies installed in the switch, an alarm triggers if a power supply fails. The alarm is automatically cleared when both power supplies are working.
SD-Card Corrupted	Enabled when an SD card DOSFS corruption is detected.
SD-Card Files Corrupted	Enabled when the IOS image specified in the SD Card system boot path is corrupted.
SD-Card Not Present	Enabled when the SD card is removed and cleared when the SD card is inserted.
SD-Card Not Supported	Enabled when an unsupported SD card is detected.
Temperature-Primary High	The primary high temperature alarm triggers at a high temperature of 203°F (95°C).
Temperature-Primary Low	The primary low temperature alarm triggers at a low temperature of -4°F (-20°C).
Temperature-Secondary High	The secondary high temperature alarm triggers when the system temperature is higher than the configured high temperature threshold.
Temperature-Secondary Low	The secondary low temperature alarm triggers when the system temperature is lower than the configured low temperature threshold.
Device Status	
Device Boot Configuration Failed	This indicates there has been a failure in applying device boot configuration. It gets cleared when the device is successfully moved to licensed state.
Device Startup Configuration Changed	This indicates that the device startup configuration has changed.
Device Unreachable	This indicates that the device is unreachable from IND. It gets cleared when the device is reachable.
Licensing	
License expired	This denotes expiry of Classic IND Licenses for the devices. It gets cleared when the user gets new licenses generated.

Alarm Name	Description
License is out of compliance	This is generated when smart licenses are in shortage. It gets cleared when more licenses are added.
License violated	This alarm is triggered if the license for a licensed device is expired. It is cleared when licenses are renewed. Applicable for both classic and smart licensing.
License will expire in less than 15 days	This alarm is triggered if a classic license is going to expire in 15 days. This alarm is cleared on license renewal.
Port Status	
FCS Error	The switch generates an FCS bit error-rate alarm when the actual FCS bit error-rate is close to the configured rate. You can set the FCS bit error-rate by using the interface configuration CLI for each of the ports.
Half-Duplex Port Detected	This alarm is raised when half-duplex mode is detected on a port. It is cleared after both sides select full-duplex mode.
Interface Down	This alarm is generated when any interface is down. It is cleared after the interface is back up.
Link Fault	The switch generates a link fault alarm when problems with a port physical layer cause unreliable data transmission. A typical link fault condition is loss of signal or clock. The link fault alarm is cleared automatically when the link fault condition is cleared.
Port Down	The switch generates this alarm when any port is down. The alarm is cleared after the port is back up.
Port Failure	The switch generates this alarm for any port failure. This alarm is cleared when the port returns to normal state.
Port Not Forwarding	The switch generates a port not-forwarding alarm when a port is not forwarding packets. This alarm is cleared automatically when the port begins to forward packets.
Port Not Operating	The switch generates a port not-operating alarm when a port fails during the startup self-test. When triggered, the port not-operating alarm is only cleared when the switch is restarted and the port is operational.
Redundancy	

Alarm Name	Description
DLR Partial Network Fault	A network fault has been detected in one direction only. This fault occurs only when the node is the active ring supervisor.
DLR Rapid Fault Restore Cycle	A series of rapid ring fault/restore cycles has been detected. Similar to the Partial Network Fault status, the supervisor remains in a state with forwarding blocked on its ring ports. This alarm is cleared when the ring returns to normal state.
DLR Ring Fault	A ring fault has been detected. This alarm is cleared when the ring returns to normal state.
DLR Unexpected Loop Detected	A loop has been detected in the network. This alarm is cleared when the ring is restored.
MRP Manager Change	This alarm is triggered when there is a MRP Manager Role change in the discovered topology.
MRP Ring Open	In the case of failure of a link connecting two MRCs, both ring ports of the MRM change to the forwarding state, the MRCs adjacent to the failure have a blocked and a forwarding ring port, and the other MRCs have both ring ports forwarding. If MRP Manager is a PLC, there is no MRP Ring Open alarm.
PRP Channel Interface Down	This alarm is triggered when the port status of either of the ports in a PRP channel is down.
PRP Warning Count Seen On LAN-A	This alarm is triggered when there is an increase in the warningCount seen on LAN-A. This alarm is cleared if there is no increment in the warningCount in the next periodic data refresh.
PRP Warning Count Seen On LAN-B	This alarm is triggered when there is an increase in the warningCount seen on LAN-B. This alarm is cleared if there is no increment in the warningCount in the next periodic data refresh.
PRP Warning Seen On LAN-A	This alarm indicates any potential problem on the PRP port, such as a port not receiving the Link Redundancy Entity (LRE) frames within the stipulated time. This alarm is triggered based on the ingress counter of the same name: ingress warning lan a.
PRP Warning Seen On LAN-B	This alarm indicates any potential problem on the PRP port, such as a port not receiving the Link Redundancy Entity (LRE) frames within the stipulated time. This alarm is triggered based on the ingress counter of the same name: ingress warning lan b.

Alarm Name	Description
REP Port Failed	This alarm is triggered when there is a port failure in the REP segment. This alarm is cleared after the port is up.
REP Segment Non Operational	This alarm is triggered when the REP port is down,flapping, and so on. It is cleared after the port returns to normal state.
REP Segment Preempt Failed	This alarm is triggered when pre-emption of a segment failed despite the trigger being successful. It is cleared after the pre-emption is successful.
REP Segment Preemption Trigger Failed	This alarm is triggered when the pre-emption triggered on the REP primary edge failed. If the trigger is successful the next time, this alarm is cleared.
STP Loop Inconsistent	This notification indicates that an STP loop is inconsistent. It is cleared when the loop is consistent.
STP New Root Elected	This notification indicates that a device is elected as the new root for STP.
STP Port Inconsistent	This notification indicates that the STP port is inconsistent. It could be because of port type mismatch or PVID mismatch. This alarm is cleared after the condition becomes normal.
STP Root Inconsistent	This notification indicates that the STP root is inconsistent due to erroneous configuration. After it returns to normal, the alarm is cleared.
STP Topology Changed	This notification indicates that a topology change has occurred in the STP tree.
Security	
Message From Unknown Device	This notification indicates messages were received from an unknown device (that is, a device not in IND inventory).
System Status	
Backup Failed	This notification indicates Backup has failed. After the backup is successful, this alarm is cleared.
Cisco Active Advisor Upload Failed	This notification indicates that IND was unable to send network information to Cisco Active Advisor. On successful update of CAA, this alarm is cleared.
Time Services	

Alarm Name	Description
PTP Grandmaster Clock Changed	This notification indicates that the device is no longer a Grandmaster. After the status is restored, this alarm is cleared.
PTP Grandmaster Not Found	This notification indicates that this device is no longer being served by any Grandmaster. After the GrandMaster is restored, the alarm is cleared.
PTP GrandMaster Offset Threshold Exceeded	The value for Offset Threshold From Grandmaster has exceeded the configured value.
PTP Master Clock Changed	This notification indicates that this node is being served by a different Master. After the configuration is restored, this alarm is cleared.
PTP Steps Removed From Grandmaster Changed	This notification indicates that the number of steps from Grandmaster to this device changed. After the number is restored, the alarm is cleared.

Backup

A backup is a set of compressed files that can be restored to return the system to a particular point in time. A backup is stored on the local system or a remote repository such as a network drive from which you can download the files. The backup is a full (not incremental) backup and contains all the necessary files to restore the system if needed.

A backup can be scheduled as a periodic backup or can be invoked as an on-demand backup. If a backup is scheduled, the schedule is displayed at the top of the **Settings > Backup** page.

- Click **Location** to specify the path to the backup and click **Save**.
- Click **Schedule** to schedule a periodic backup. Only one periodic backup task will be scheduled in the system. If you change the schedule, the existing periodic task will be rescheduled to the new schedule.
In the Schedule Backup pop-up window, select a day of the week or month and the time of day for the backup, and click **Save**. Click **Remove** to remove a backup schedule.
- Click **Backup Now** to begin a backup immediately.

File Name	<p>Name of the backup in the format <code>ind_backup_mmddyy_hhmmssms_version.zip</code> (for example, <code>ind_backup_081516_094102493_1.0.0.zip</code>), where:</p> <ul style="list-style-type: none"> • <code>mmddyy_hhmmssms</code> (month, day, year, hour, minute, second, and millisecond) is the time when the backup is taken. Millisecond can be two or three digits. • <code>version</code> is the system version.
-----------	---

Created Time	Time when backup file was created.
Size	Backup file size.
File Location	The path to where the backup file is stored. The location can be a local disk such as the C:\ or D:\ drive or a remote mounted location such as E:\ or F:\.
Backup Status	Outcome of the backup: Failed or Successful.

Certificate Management

A certificate is an electronic document that identifies an individual, a server, a company, or other entity and associates that entity with a public key. A self-signed certificate is signed by its own creator. Certificates can be self-signed or digitally signed by an external Certificate Authority (CA). A CA-signed digital certificate is considered industry standard and more secure.

Certificates are used in a network to provide secure access. IND uses certificates for secure device communication, PnP, and for communicating with external services such as pxGrid.

You can manage these types of certificates:

- System Certificate:

IND system certificates are server certificates that identify a Cisco IND server to devices and to clients in the deployment. System certificates are:

- Used by browser (WEB UI) and REST clients who connect to the IND web server.
- Used by pxGrid (ISE) to communicate with IND.
- Used by IOS Devices (PnP agent) to communicate with the IND (PnP server).
- Used by OPC UA devices to communicate with the IND web server.

- Trusted Certificate:

The Trusted Certificates Store contains X.509 certificates that are used for trusting the clients connecting to the IND web server. IND uses the trusted certificates for the following purposes:

- To verify client certificates of pxGrid (ISE).
- To verify client certificates of IOS devices.
- To verify client certificates of OPC UA devices.
- To verify client certificates of the Cisco ASD Server.

You can use **Settings > Certificate Management** to manage certificates.

- System Certificates
- Trusted Certificates
- Settings

Click the **System Certificates** or **Trusted Certificates** menu tile on the left of the Certificate Management page to view and manage System or Trusted Certificates.

To replace a certificate, select it in the System Certificates or Trusted Certificates table, click **With Selected**, and then click **Delete** to delete the existing certificate. Add the new System Certificate or Trusted Certificate as described below.

Click **Settings** (described below) to select a Self-Signed or CA certificate for each of the services in the system.

Field	Description
Name	Name of the certificate.
Issued To	Distinguished Name (DN) of the computer, user, network device, or service that the CA issues the certificate to. The name is commonly represented by using an X.500 or Lightweight Directory Access Protocol (LDAP) format.
Issued By	DN of the CA that issued the certificate. The name is commonly represented by using an X.500 or LDAP format.
Valid From	The date and time when the certificate becomes valid.
Certificate Expiry	The date and time when the certificate is no longer considered valid. The date when an application or service evaluates the certificate must fall between the Valid From and Valid To fields of the certificate for the certificate to be considered valid.
Download Certificate	(System certificates only) Click the button to download the certificate and open it for viewing or save it to your system.
Certificate Type	Specifies whether the certificate is Self Signed or CA Signed.

Adding System Certificates

To add a system certificate:

1. Click the **System Certificates** menu tile on the left of the Certificate Management page.
2. Click **Add Certificate**.
3. In the Add System Certificate pop-up window, enter a name for the certificate.
4. Click **Browse** to select the certificate.
The file must have a valid X.509 certificate format such as PEM, CER, DER, PFX, or PKCS12.
5. Click **Browse** to select a private key. Supported formats for private key are PEM and CER.
6. Enter a password for the certificate.

For PKCS12/PFX certificate type, the password field is mandatory. For PEM/CER/DER certificate type, the private key is mandatory and among this some private key requires password.

Adding Trusted Certificates

To add a trusted certificate:

1. Click the **Trusted Certificates** menu tile on the left of the Certificate Management page.
2. Click **Add Certificate**.
3. In the Add Trusted Certificate pop-up window, enter a name for the certificate.
4. Click **Browse** to select the certificate.

The file must have a valid X.509 certificate format such as PEM, CER, DER, PFX, or PKCS12.

5. Enter a password for the certificate.

Settings

Click the green toggle button to select a Self-Signed or a CA certificate for pxGrid, PnP/Web UI, and OPC UA.

If you choose to use a CA certificate, select the certificate from the drop-down menu.

Device Pack

Device Pack is a set of files that you use to add support for new device types to the system. Device support that is separate from the core system application makes it easier to add device types to the system after initial installation. You can install a new Device Pack without having to restart the system.

Device Pack can only be installed in the system with a matching version number, and the release number must be the same or greater than the system release number. For example, in 1.0.0-180, 1.0.0 is the version and 180 is the release number. A new Device Pack must have version 1.0.0 and the release can be 180 or higher.

The **Settings > Device Pack** page displays the current version and release number of the installed Device Pack and when it was installed. To install a new Device Pack, click **Install New Device Pack**.

Group Management

Use the **Settings > Group Management** page to create groups to which you can assign devices. You can assign devices from the Licensed Devices and All Devices categories to a group and organize groups of devices in a hierarchical structure. You can create up to 1000 groups. The maximum number of siblings is 100, and each sibling can have 10 child groups. The groups that you create and their placement in the hierarchy are displayed in the left pane.



Note You can view groups in a topology map as described in [Topology, on page 80](#).

Groups are mandatory; that is, an asset must be assigned to a group. The system creates a default root group to which devices are assigned, unless a different group is specified during Asset Discovery. You can move devices from the Root group to other groups as described below.

The system-defined root group is the root group in the group hierarchy and is named "Root" by default. You can rename the system-defined root group but you cannot delete it. You can delete a child group only when there are no devices associated with it.

- To change a group's placement in the hierarchy, click on the group in the left pane and drag and drop it to the new placement.
- Click **Add Group** to add a new group. Enter the name and description and click **Save**.
 - The name can be from 1 - 20 characters long and can contain the following characters: A-Z, a-z, 0-9, underscore (_), and dash (-). The name cannot start or end with underscore (_) or dash (-).
- To edit or delete a group, select the group in the left pane and click **Edit** or **Delete**.



Note You cannot delete a group if it is associated with a PnP Profile (see [Profiles, on page 10](#)).

- Click an existing group name in the left pane to display group details in the right pane. Group details include the total number of devices in this group, the number of devices in group hierarchy, the total number of subgroups in the group hierarchy, group description, and table of devices in the group.
- Click the Name link in the Devices table to view [Device Details, on page 48](#).
- Click the Connected To links in the Devices table to view details for the device or port that the device is connected to.
- To move device(s) between groups (for example, from the Root group to a group that you created), select the device(s) in the table in the right pane and click **With Selected**. Select a group from the Move Device(s) to Group drop-down list, and then click **Yes** to confirm the move.

Name	The name of the device. Click the link to display the device overview.
Product ID	Product Identifier
Device Type	Type of device (for example, switch).
Vendor	Name of the manufacturer of the device.
IP Address	Internet address of the device in dot-decimal notation.
MAC Address	MAC address of the device.
Connected To	Device(s) connected to this device. Click the link for the connected device to display the device details. Click the link for the connected interface to display the interface details.


Tags	<p>The tags associated with this device.</p> <ul style="list-style-type: none"> • If tags are associated with this device, the tag names are displayed as a link. Click the link to display the Associated Device Tags pop-up window to add or remove tags. • If no tags are associated with the device, + is displayed as a link. Click the link to display the Associated Device Tags pop-up window to add or remove tags.
------	--

Licenses

Use the **Settings > Licenses** page to manage your Industrial Network Director (IND) licensing. You can use Classic Licensing or Smart Licensing.

- Classic Licensing is Cisco's legacy licensing model based on Product Activation Keys (PAK) and Unique Device Identifiers (UDI).
- Smart Licensing is a cloud-based approach to licensing and is the default licensing mode when IND starts up.



Click  to change the licensing mode from Smart Licensing to Classic Licensing.

IND enforces licensing as follows:

- A valid license is required to manage Licensed devices in the Licensed state.
 - License status is displayed in a red box at the top right of the IND window. Users with System Administrator permissions can click this button to go to the **Settings > Licenses** page.
 - No status is displayed if there is a valid license.
 - License Violation is displayed if there are no licenses in the system.
 - Evaluation License is displayed if there is an evaluation or demo license in the system.
- IND warns you before the license expires.
- When no valid licenses are found, devices in Licensed state are automatically moved to the Unlicensed state.
 - IND raises a critical event when it moves devices to the Unlicensed state.
 - The **Operate > Inventory** page displays devices in Unlicensed state that have an expired license.
 - After adding a new license or renewing a license, you need to manually move the devices to Licensed state.
- You need to manually close open license alarms.

Table 16: Licensing Usage

License Type	A description of the license; for example, IND Smart License for Managing IE switches.
Status	Displays whether license is Authorized, Evaluation, Out of Compliance, Authorization Expired, Evaluation Period Expired, or No Licenses in Use.

Classic Licensing

In Classic (Traditional) Licensing, you receive a Product Activation Key (PAK) for each order and UDI (Host ID) information of the host where the software is installed.

The Host ID is displayed on the **Settings > Licenses** page when Smart Licensing is disabled. You input the PAK and host ID into the Cisco Licensing tool to generate the license, Cisco emails you the license file, and then you can import the license file to IND.

- Click **Switch to Smart Software Licensing** to use Smart Licensing instead of Classic Licensing.
- Click **Import License Files** to select a license file from your PC to import to IND.
- To delete license files, select the files in the list, click **With Selected**, and then click **Delete**.

Table 17: Device(s) Summary

Host ID	A system-generated SHA-1 hex string that is a combination of the device UUID and volume serial number.
License Type	A description of the license; for example, Industrial Ethernet Switch.
Total	The total count of the given license type that is available in the system.
Used	The count of the given license type that is currently being used in the system.

Table 18: License File(s)

File Name	Name of the license file.
File ID	A unique ID to identify the license file.
PAK	Product Authorization Key (PAK) number from the license file.
Added At	Date when the license file was added.
Expiration Date	Date when the license file expires.

License Mode	Shows Demo if this is a demo license. If this is a regular term license, nothing is shown.
--------------	--

Smart Licensing

With Smart Licensing, you use your Cisco account to purchase entitlements through Cisco Commerce Workspace (CCW). The entitlements are immediately deposited into your Virtual Account for usage, eliminating the need to manage license files in the system. You can manage your Cisco software licenses from a single location, the Cisco Smart Software Manager (CSSM), which you can access over a direct Internet connection or by using the CSSM satellite application installed at your premises. For more information, see [Cisco Smart Accounts](#).

- Click **Register** or **Reregister** to register the product for Smart Software Licensing. A token is required to register the product. Registration tokens are generated using the CSSM and are stored in the Product Instance Registration Token Table that is associated with your smart account. Copy and paste the token into the field in the Smart Software License Registration pop-up window.

Click the **Direct** link if you want to change transport settings (see Transport Settings below), and then click **Register**.

- Click the link for [Smart Software Manager](#) to view and manage Smart Licenses for your Cisco Smart Account.

Table 19: Licensing Status

Registration Status	Displays whether license is Registered, UnRegistered, or Registration Expired, and the time of registration.
License Authorization Status	Displays whether license is Authorized, Evaluation, Out of Compliance, Authorization Expired, Evaluation Period Expired, or No Licenses in Use, and the time of authorization.
Smart Account	The name of your Smart Account.
Virtual Account	The name of the Virtual Account that the product was registered with.
Product Instance Name	The unique identifier for a single running instance of the product.

Transport Settings	<p>Select how you want to transfer licensing information:</p> <ul style="list-style-type: none"> • Direct Connection to Cisco Licensing Server—Transfer usage over the Internet to the cloud server directly from the system to the cloud via HTTPS. • Transport Gateway - proxy data via Transport Gateway or Smart Software Manager satellite—Periodically transmit the information into the cloud using periodic network synchronization. Enter the URL of the Transport Gateway or Satellite. • HTTP/Https Proxy - Send data via an intermediate HTTP or HTTPS proxy—Transfer files directly over the Internet to the cloud server through an HTTPS proxy, either Smart Call Home Transport Gateway or off the shelf HTTPS proxy such as Apache. <ul style="list-style-type: none"> • Enter the IP address and port number of the HTTP or HTTPS proxy. • Enter an optional username and password configured for the proxy server.
--------------------	--

Policy Servers

Use the **Settings > Policy Servers** page to configure external AAA (Authentication, Authorization and Accounting) or Policy servers for user authentication and authorization. Policy servers can use the RADIUS or PxGrid protocols.

You can configure the authentication mode for users on the **Settings > Users > External Authentication** page. You can also configure a primary and a secondary AAA server and whether to fall back to local database authentication if all configured AAA servers are down or unreachable. See [External Authentication, on page 122](#) for information about these settings.

- To add a server, click **New**, configure settings, and click **Save**.
- To edit server settings, click the link under Host Name, configure settings, and click **Save**.
- To delete a server, select it from the list, click **With Selected**, and then click **Delete** in the pop-up window.

Protocols	<p>Check the check box to select the protocols supported by the Policy server.</p> <ul style="list-style-type: none"> • RADIUS: This Policy server will be used as AAA server under Settings > Users > External Authentication. • pxGrid: If pxGrid is enabled, this policy server will be used as the ISE server under Settings > pxGrid.
Simple, Advanced	<p>(RADIUS only)</p> <p>Click the green toggle button to display or hide expanded settings for the RADIUS server.</p>
Host Name	Name of the Policy server.
IP Address	IP address of the Policy server.
Description	Optional description for the Policy server.
AAA Settings (RADIUS only)	
Retries	<p>The number of times for the client to attempt authentication.</p> <p>Range is 1-3. Default is 1.</p>
Timeout	<p>Time interval for the client to wait for a response.</p> <p>Range is 2 to 30 seconds. Default is 3 seconds.</p>
Authentication Port	<p>The UDP destination port for authentication requests.</p> <p>Default is port 1812.</p>
Shared Secret	<p>Enter a string to be used to authenticate transactions between the system and the RADIUS server:</p> <ul style="list-style-type: none"> • The shared secret you enter must match the shared secret configured on the AAA server. • The length of the string must be at least 5 characters. <p>Note The stored shared secret is encrypted.</p>

pxGrid

Cisco Identity Services Engine (ISE) is a network administration product that enables the creation and enforcement of security and access policies for endpoint devices connected to the company's routers and switches.

ISE uses Platform Exchange Grid (pxGrid) technology to share rich contextual data with integrated technology partner solutions. pxGrid is an Internet Engineering Task Force (IETF) standards-driven data-sharing and control platform. IND uses pxGrid to share information about Other devices available in its inventory with ISE.

pxGrid is disabled by default. To configure IND for pxGrid:

1. The **Settings > pxGrid** page displays the option **Download .pem certificate**. Click the button to download the IND certificate in Privacy Enhanced Mail (PEM) format to import to ISE.

Import this certificate on ISE under Administration > System > Certificates > Trusted Certificates.

This certificate is required for pxGrid Registration and for ISE to bulk download IND assets (Endpoints) onto ISE.

2. Click the **Settings > Certificate Management > Trusted Certificates** menu tile on left of pxGrid page, and then click **New** to upload the ISE trusted certificate. In the Upload Trusted Certificate pop-up window, click **Browse** to select the ISE Server trusted certificate.

Trusted certificates are the ISE certificates imported into IND to enable verification and trust of ISE during SSL communication.



Note ISE trusted certificates can be uploaded or deleted only when pxGrid is in Disabled state.

3. On the PxGrid Settings page, click the green toggle button to enable pxGrid.



Note The button to enable or disable pxGrid is available only before the pxGrid node is registered.

4. On the pxGrid Settings page, select whether to connect to ISE using an existing node or register a new one. To register a new node, enter the information for the ISE server described in the table below and click **Register**.

Once registered, if manual approval is needed on the ISE Server, you can activate pxGrid on IND only after the pxGrid node is approved on the ISE Server. If auto approval is enabled on the ISE Server, pxGrid will be activated automatically after registration.

5. Click **Activate** to activate the pxGrid service on IND.

After activation, IND will push real-time asset notifications to ISE, and ISE can pull information about endpoints discovered on IND.

Table 20: pxGrid Settings

ISE Server	
Node Name	Enter a name to identify this IND system as a pxGrid node in the ISE Server.
Server 1	DNS name of the primary ISE Server. The listed servers are the Policy servers that have the pxGrid protocol enabled.

Server 2	DNS name of the secondary ISE Server. The listed servers are the Policy servers that have the pxGrid protocol enabled. IND will use this server if the primary ISE server is not reachable or does not respond.
Statistics	
Sync. Status	The current pxGrid Sync Status (In Sync, Out of Sync, or Disabled).
Last Sync. Status Probe Time	Last time when IND received the request for Sync Status. This indicates if ISE is probing IND every 5 minutes.
Number of Assets Shared via Last Bulk Request	The number of assets that IND sent as part of a Bulk Request response.
Last Bulk Request Time	Last time when IND sent all the assets as part of a Bulk Request response.
Last Update Operation	Operation type of the last update sent from IND to ISE (Add, Delete, or Update).
Last Update Time	Last time at which the Asset Update was sent.
Total pxGrid Asset Count	Total count of pxGrid Assets in IND .

Table 21: Trusted Certificates

Name	Name of the ISE Server trusted certificate. The certificate can be in PKCS12, PEM, or CER format. You can specify a CA generated certificate that is trusted by ISE, or you can generate the certificate for the pxGrid client from the ISE Server on the Administration > pxGrid Services > Certificates tab. You can also upload the root certificate of the certificate used on ISE for pxGrid services.
File Name	Certificate file name.
File Size	File size of the certificate.
File Type	The format of the certificate: PKCS12, PEM, or CER.

Disabling pxGrid

Click the green toggle button on the **Settings > pxGrid** page to disable the pxGrid service on IND.



Note The registration persists if you disable pxGrid. Disabling the pxGrid service on IND will not delete the pxGrid node on ISE; the ISE Administrator needs to manually delete the IND pxGrid node on ISE.

The next time you enable pxGrid, you can connect with the existing node or register a new node.



Note If the IND server Host ID changes, the IND certificate used for pxGrid is regenerated and a warning message is displayed (after the login screen and on the pxGrid settings page). Import this newly generated IND pxGrid certificate on ISE and register a new node (follow the steps above to configure IND for pxGrid).

System Settings

Use the **Settings > System Settings** page to modify the settings that the system uses for data retention, data collection, log levels, security, email of alarm alerts, and Cisco Connection Online (CCO) account.



Note A CCO account is required for certain activities on Cisco.com. IND maintains one CCO account that it uses for CAA (Cisco Active Advisor). You can also find a link to register for a CCO account or modify CCO account settings on the [Cisco Active Advisor, on page 89](#) page.

Click the menu tile for the settings you want to change. Select new values and click **Save**.

Table 22: Data Retention

Alarm History	Number of days, from 1 - 31, that the system keeps alarms data. The default is 7.
Audit Trail History	Number of days, from 1 - 365, that the system keeps audit trail data. The default is 180.
Event History	Number of days, from 1 - 31, that the system keeps event data. The default is 7.
Metrics History	Number of days, from 1 - 31, that the system keeps metrics data. The default is 7.
Tasks History	Number of days, from 1 - 31, that the system keeps tasks data. The default is 7.
Remote Users History	Number of days, from 180 - 360, that the system keeps remote users with last successful login. The default is 180.

Table 23: Data Collection

Basic Inventory	Time interval (15, 20, or 30 minutes, or 1, 2, 3, 4, 6, 8, 12 or 24 hours) that the system performs inventory polling. The default is 24 hours.
Inventory Status	Time interval (15, 20, or 30 minutes, or 1, 2, 3, 4, 6, 8, 12 or 24 hours) that the system polls the status of inventory. The default is 15 minutes.
Metrics Statistics	Time interval (15, 20, or 30 minutes, or 1, 2, 3, 4, 6, 8, 12 or 24 hours) that the system performs metrics polling. The default is 30 minutes.
Metrics Status	Time interval (15, 20, or 30 minutes, or 1, 2, 3, 4, 6, 8, 12 or 24 hours) that the system polls the status of metrics. The default is 15 minutes.

Table 24: Log Levels

Application Log Level	<p>Sets the severity level of application messages to control the type of messages displayed.</p> <ul style="list-style-type: none"> • Debug—Debugging messages • Error—Error conditions • Info—Informational messages only • Trace—Trace messages • Warn—Warning conditions
Module	Select a module or modules from the list, and then click With Selected to configure the log level for the selected module(s).
Level	<p>The severity level of messages to control the type of messages displayed:</p> <ul style="list-style-type: none"> • Debug—Debugging messages. • Error—Error conditions. • Info—Informational messages only. • Not set—The module uses the value set at the application log level. • Trace—Trace messages. • Warn—Warning conditions.

Table 25: Accounts

CCO User Name	Your Cisco Connection Online user name.
CCO Password	Your Cisco Connection Online password. Reenter this password in the Confirm Password field.

Table 26: Security Settings

SSL Security Level	Set the SSL encryption strength for Plug-n-Play and Web UI services to Strong or Weak .
--------------------	---

Table 27: SMTP Settings

From Email	Email address that the SMTP server accepts
Authentication	Select to provide a password of 'From Email' address required for authenticating with SMTP server, and then confirm the password.
Redundancy	Select to specify a Backup SMTP Server. Enter the IP address or host name of the Backup server and port number.
SMTP Server	IP address or host name of the SMTP server.
Port	Port number on which the SMTP service runs. The default is 587.
Test Now	Click to test the SMTP settings by having the system send a test email. The system sends the test email to the email address configured in User Profile Settings, on page 126 for the currently logged in user.

Table 28: System Settings

System ID	Name of the IND application instance running on the system. By default, the value is set to the host name of the system where the IND server is running. This field is mandatory and cannot be empty. The maximum length is 255 characters and all characters are allowed except angle brackets (< and >).
Building	This field is optional and can be empty. The maximum length is 100 characters and all characters are allowed except angle brackets (< and >).

Area	This field is optional and can be empty. The maximum length is 100 characters and all characters are allowed except angle brackets (< and >).
Location	This field is optional and can be empty. The maximum length is 100 characters and all characters are allowed except angle brackets (< and >).
Region	This field is optional and can be empty. The maximum length is 100 characters and all characters are allowed except angle brackets (< and >).
Country	This field is optional and can be empty. The maximum length is 100 characters and all characters are allowed except angle brackets (< and >).
System Description	This field is optional and can be empty. The maximum length is 255 characters and all characters are allowed.

Tags

A tag is a string applied to an entity in the system. Tags are used to label devices in the system inventory. After you have tagged devices, you can use the tags for searching and filtering devices in different system views. Use the [Tags](#) page to create tags. After you create tags, you can associate the tags to devices on the [Inventory](#), [on page 38](#), [Device Details](#), [on page 48](#), [Topology](#), [on page 80](#), [Configuration Archives](#), [on page 90](#), or [Group Management](#), [on page 103](#) pages.

There are two kinds of tags:

- Regular—Not published through pxGrid.
- Security—Published through pxGrid.

IND publishes the tag to an identity-based network access control and policy enforcement system such as Cisco Identity Services Engine (ISE) as a custom attribute through pxGrid. An authorization policy can be applied based on this security tag custom attribute.

Security tags allow dynamic changes in security policy across the network. For example, a device may be assigned security tag X that maps to Secure Group Tag (SGT) 10, which allows the device to communicate only within cell-1. The security tag assigned to the device could be changed to security tag Y, which maps to SGT 100 and allows access from the upstream firewall for remote maintenance.

You must have Device Management administrative rights to Add/Delete/Assign/Unassign Regular tags. You must have Security Management administrative rights to Add/Delete/Assign/Unassign Security tags (System Administrator and Network Administrator roles inherit Security Management permissions by default).

- To create a new tag, select **Regular** or **Security** in the left pane, then click **New**.

You can create up to 50 device type tags (includes Regular and Security). You cannot change the tag category between Regular and Security after you create the tag.

- To delete a tag, select it from the list in the table, click **With Selected**, and then click **Delete** in the pop-up window.

You cannot delete a tag if it has associated devices.

- To see the devices associated with a tag, click the link in the Associated Devices column.

Name	The name that you assign to the tag. The maximum length is 50 characters and spaces are not allowed.
Associated Devices	The device(s) associated with this tag. This column is empty if there are no devices associated with this tag. A device can have up to 5 regular tags and 1 security tag.

Users

Use the **Settings > Users** page to modify the settings that the system uses for user accounts, user roles, active sessions, password policies, and external authentication. Click the menu tile for the settings you want to change.

User Accounts

Use the **Settings > User Accounts** page to add new local users to the system and view the list of currently configured users.

- Click **Add New User** to create a new user account.
- To edit an existing user account, click the link in the User ID column.
- Select user IDs from the list of existing users and click **With Selected** to delete the selected user accounts. You can also change the status or the role for the selected user accounts. The following users cannot be deleted: 1. System Admin user. 2. Active users. 3. If an open alarm is assigned to the user.

Table 29: New User Account/Edit User Account

User ID	The user ID for this account. The user ID can contain only alphanumeric characters (A-Z, a-z, 0-9, _) and can be 4-32 characters long.
---------	---

Name	<p>The name of the user for this account.</p> <p>The name can be from 1 - 50 characters long and can contain the following characters: A-Z, a-z, 0-9, underscore (_), dash (-), spaces, and all non-ASCII characters. The name cannot start or end with underscore (_), dash (-), or spaces.</p>
Account Status	Select whether the account is Active or Disabled.
Role	Select a role for this user from the drop-down list. Roles are configured on the Settings > User Roles page.
Password, Reset Password	<p>The password for this username.</p> <p>Note You must have User Management privilege on the system to change a user's password. You will also be prompted to enter your own password.</p> <p>The password must meet the requirements defined by the password policies (see Password Policies, on page 120). By default, the password must be at least 6 characters and contain the following:</p> <ul style="list-style-type: none"> • A lowercase character: a-z • An uppercase character: A-Z • A numeric character: 0-9 • A special character: --!@#%*_+=`(){};:", .?/^&<> \ []

User Roles

User authorization to perform specific tasks is controlled by the Role assigned to the user.

Three roles are pre-defined on the system:

- Network Administrator: User in this role has permissions to manage network resources.
- Operator: User in this role has permissions to monitor the network.
- System Administrator: User in this role has all the available permissions on the system.

The permissions available in IND are described below.

Permission	Description
Alarm Management	<p>Allows you to perform the following operations:</p> <ul style="list-style-type: none"> • Manage events and alarms. • Set the threshold for PTP alarm generation.

Permission	Description
API Tool	Allows you to view and use the Swagger tool.
Configuration Management	Allows you to manage configuration archives for the supported devices.
Device Management	Allows you to perform the following operations: <ul style="list-style-type: none"> • Manage and monitor devices, including tasks such as topology, inventory, and data refresh. • Manage Access Profiles. • Manage software images. • Manage DHCP. • Troubleshoot using SNMP and other diagnostic tools.
Discovery	Allows you to perform the following operations: <ul style="list-style-type: none"> • Manage Discovery Profiles and initiate discovery. • Manage PnP. • Manually add devices to the inventory.
Network Settings	Allows you to perform the following operations: <ul style="list-style-type: none"> • Manage Groups. • Manage Alarm Settings.
Port Settings	Allows you to configure ports for supported devices.
Security Management	Allows you to manage Security Tags.

Permission	Description
System Settings	<p>Allows you to perform the following operations:</p> <ul style="list-style-type: none"> • Edit system settings such as data settings, pruning settings, and security settings. • Manage licensing, including core and smart licensing. • Manage backup settings. • Manage IND software update. • Manage PxGrid settings. • Manage certificates. • Configure Policy server and SMTP server. • Manage Cisco Connection Online (CCO) settings. • Manage Cisco Active Advisor (CAA) settings. • Manage Device Pack.
User Management	Allows you to configure and manage roles, permissions, users, audit trails, external authentication, and password policies.
View Only	Allows read-only operations on IND.

To configure User Roles:

- Click **New User Role** to create a new role.
- Click **View *x* Users with this role** to see the account information in **Settings > User Accounts** for the user(s) with this role.




- Click  to edit or delete a role.
- Assign users to roles on the **Settings > User Accounts** page.

Table 30: New User Role

Role Name	<p>Name for this user role.</p> <p>The name can be from 1 - 50 characters long and can contain the following characters: A-Z, a-z, 0-9, underscore (_), dash (-), spaces, and all non-ASCII characters. The name cannot start or end with underscore (_), dash (-), or spaces.</p>
-----------	--

Role Description	Description for this user role. The description can be from 1 - 255 characters long and cannot contain "<" or ">".
Administrative Rights	Check the check boxes for the functions that you want users in this role to perform. The View Only permission is selected by default for all roles and cannot be changed.

Active Sessions

Use the **Settings > Users Active Sessions** page to view information for all active sessions of both local and remote users. At any given time, a user can have a maximum of 5 active sessions.

- To forcefully log out another user, select the user from the list and click **With Selected**. Click **Force Logout**.



Note Only the System Administrator role has permission to forcefully log out a user.

User ID	The user associated with the session. The entire row denoting the current session is grayed out, and the user ID column shows the user ID of the current user, followed by (Current Session). The row is grayed out because the user cannot kill the current session and must sign out instead.
Remote User	Indicates if the user is a local user or remote user.
Login	Time when the user logged in.
Last Accessed At	Time when the user last accessed the system.
IP Address	Client IP address.

Password Policies

Password policies dictate the strength, reuse, and lifetime of the passwords used by users to access the system. You can customize the password policies to meet a desired security posture.

By default, all Password Policies are enabled except for Max Failed Password Retry Attempts, which is disabled by default. Click the green toggle button to disable or enable any of the policies. You can modify the parameters within the ranges specified in the form fields.

Numeric Character Policy	Password must contain a numeric character. Range: 0 - 9
--------------------------	--

Lowercase Character Policy	Password must contain a lower case character. Range: a - z
Special Character Policy	Password must contain a special character. Range: ~!@#%* _+=\ (){};":'/?^&<> \[\]
Uppercase Character Policy	Password must contain an upper case character. Range: A - Z
Password Expiry Policy	Defines the period (in days) after which the password expires. <ul style="list-style-type: none"> • Minimum: 40 • Maximum: 1825 • Default: 180
Password Expiry Warning Period	Defines the length of time (in days) before the password expiration date to provide a warning message. <ul style="list-style-type: none"> • Minimum: 15 • Maximum: 30 • Default: 30
Max Failed Password Retry Attempts	Defines the maximum number of incorrect attempts allowed in the retry period, after which the user account is locked. <ul style="list-style-type: none"> • Minimum: 5 • Maximum: 10 • Default: 5
Password Length	Defines the minimum characters each password must contain. <ul style="list-style-type: none"> • Minimum: 6 • Maximum: 127 • Default: 6
Password Reuse Policy	Defines the number of most recent passwords of the user that cannot be reused. <ul style="list-style-type: none"> • Minimum: 0 • Maximum: 24 • Default: 5

External Authentication

Use the **Settings > Users > External Authentication** page to select the authentication mode for authenticating and authorizing IND users.

A remote user is granted access only if both authentication and authorization are successful. When authentication/authorization is attempted using a AAA server, the response from that AAA server has the User Role information. IND checks if that User Role is valid and exists on the system, and then it authorizes the user.



Note The default role *System Administrator* created by the system cannot be assigned to a remote user.

See the **Settings > Users > Active Sessions** page to display information about local and remote users that have active sessions.

Authentication Mode	Select whether to use the local database or RADIUS for authenticating users.
Primary AAA Server	Select a primary server from the drop-down list. AAA servers are configured on the Settings > Policy Servers page.
Secondary AAA Server	Select a secondary server from the drop-down list. Users are authenticated on the secondary server only if the first server is not reachable or not responding. AAA servers are configured on the Settings > Policy Servers page.
AAA Attribute Name	The name of the AAA attribute list to be used for RADIUS. This Attribute Name must match the Attribute Name configured on the AAA Server. The Attribute Value format accepted by IND is: Role=Operator The Role name must match an existing User Role in IND.
Fallback to Local	Click the toggle button to select whether to fall back to local database authentication if all configured AAA servers are down or unreachable. Note Remote users will not be able to log in to IND if the AAA Server is down or unreachable.





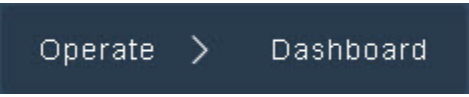
CHAPTER 6







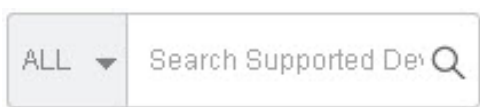


User Interface



- [Buttons and Controls](#), on page 123
- [Tasks](#), on page 125
- [User Profile Settings](#), on page 126

Buttons and Controls

Refer to the table below for descriptions of the buttons and other control elements that appear throughout the IND user interface.

	<p>Click to return to Operate > Dashboard.</p>
	<p>Use the Context Group drop-down menu to select the group you want to view. IND refreshes the display to list only devices under the selected group and below.</p> <p>By default, the group view is set to the group that you are assigned to for your IND user account (the Auth Group). You can change the group from your assigned group to any of its subgroups. This group selection is saved in your User Preferences so the same group view is displayed on other pages within IND or after you log out and log back in.</p> <p>See User Accounts, on page 116 for information about user Group assignment.</p>
	<p>Click to expand the IND menu.</p>

	<p>Shows the license status:</p> <ul style="list-style-type: none"> • No status is displayed if there is a valid license. • License Violation is displayed if there are no licenses in the system. • Evaluation License is displayed if there is an evaluation or demo license in the system. <p>See Licenses, on page 105 for more information.</p>
	<p>Shows the total number of current alarms on the system. Click to go to the Operate > Alarms page.</p>
	<p>Click to display information about tasks on the system that are running or completed. For more information, see Tasks, on page 125.</p>
	<p>Select Help, Guided Tours, Download Logs, or API Tool from the drop-down list.</p>
	<p>Click to display your user name, change your profile settings, or Sign Out. See User Profile Settings, on page 126.</p>
	<p>Click to hide or display a pane on the left of the browser window that lets you refine the display of items listed.</p>
	<p>Use the search function to search for entities in the database.</p> <ul style="list-style-type: none"> • Enter text in the text box and press enter to search for a text string. Select a field from the drop-down list to narrow the search. • Perform a wildcard search using "?" to represent a single character and "*" to represent a sequence of characters. • Perform an exact search using double quotes ("") around the word.
	<p>Click to display a pop-up window where you can perform actions on the selected items. Actions vary by page.</p>
	<p>Click to populate the page with the latest data.</p>

	Click to select the columns that appear in the table. Some columns always appear and cannot be deselected (as identified by a lighter shade of text).
	Click to display or hide passwords on pages such as User Accounts where you configure passwords.


Terminology

The following list defines terms used throughout the system user interface and this online help:

System	The Industrial Network Director application.
Licensed Device	In this release, devices are licensed based on PID and supported features. Supported PIDs/product families are listed in the release notes. These PIDs are Cisco switches that are managed by IND. Non-Cisco devices are licensed based on features that are supported on IND. Currently three features are supported: Backplane Bridging, DLR, and PTP (see Inventory, on page 38 .) A device is licensable if it supports any of these three features.
IE Switch	A Cisco Industrial Ethernet Switch.
All Devices	Category of devices that includes devices not listed in the Device Pack, as well as IE switches that are in the Device Pack. These devices are represented by various icons in the Topology map.
Licensed state	A Licensed device for which the system performs active device monitoring, including information polling, alarms, and telemetry, and that has a valid license.
Unlicensed state	A Licensed device for which the system does not perform monitoring and that does not have a license associated with it.

Tasks



Click the Tasks button  to display information about tasks on the system that are running or completed. Examples of tasks include IP Scan Discovery that runs when you click **Scan Now** on the **Operate > Asset Discovery** page, or Device State Change, which you initiate from the **Operate > Inventory** page. Tasks are made up of subtasks.

- To view details about a task, including subtasks, click the Name link.


Name	Display name of the task.
Created By	User who initiated the task.
State	State of the task: Running or Completed.
Created	Time when the task was created.
Started	Time when the task execution started.
Ended	Time when the task execution ended.

Subtask

Subtask	Display name of the subtask.
Result	The outcome of running the subtask (for example, Success or Error).
Details	Details about the subtask. Click the link to display the details in a pop-up window.
Started	Time when the subtask execution started.
Ended	Time when the subtask execution ended.

User Profile Settings



To change your user profile settings such as your password and email address, click  and then select **Profile Settings** from the drop-down menu. You can also use this page to subscribe to email alerts for alarms. Click **Save** to save your changes.

User Profile	
Username	(not editable) the user name configured for this user account in Settings > Users .
Role	(not editable) the role configured for this user account in Settings > Users .
Email	Enter an email address or update an existing email address in the system.

Reset Password	Click the toggle button to reset your password. Enter your current password, the new password, and then confirm the new password.
Alarm Notifications	
Subscribe to Email Alerts for Alarms	<p>Click the toggle button to configure receipt of email alerts for alarms generated by IND . Check the check boxes to receive alerts for Minor, Major, and Critical alarms.</p> <p>A user can subscribe for alarm notification only if the SMTP server is set up on IND . See System Settings, on page 112.</p>



CHAPTER 7

Troubleshooting

- [Installer Failures, on page 129](#)
- [Discovery Failures, on page 129](#)
- [Administrative State Change Failures, on page 131](#)
- [CIP Backplane, on page 131](#)
- [Page Not Found, on page 132](#)
- [No Permission, on page 132](#)
- [Configuration Archive Failures, on page 132](#)

Installer Failures

Please verify Windows firewall configuration and allow traffic on the following ports through the firewall:

- TCP Ports 8443, 443, 80, 21, 50000-50050
- UDP Port 30162

Discovery Failures

Follow the procedures in the following sections to troubleshoot discovery failures.

Device Discovery

If the scanned device does not appear on the **Operate > Inventory** page as a Licensed Device, do the following:

1. Check if the device appears in the All Devices category (left panel of the Inventory page). If it does, verify the following:
 - a. Verify that the device PID is in the list of Licensed devices in **Settings > Device Pack**.
 - b. Verify that the device supports DLR or PTP or Backplane Bridging features.
 - c. Verify that SNMP is enabled on your device. See [Device Prerequisite Configuration, on page 76](#) for more details.
 - d. Verify that the SNMP credentials provided on the Access Profile match the ones defined on the device.

- e. Verify that the SNMP port 30162 is not blocked on the Windows firewall.
2. If the device does not appear in either the Licensed or All Devices on the Inventory page, make sure the device IP is reachable through the system. Go to the command prompt on the Windows system where the system is running and ping the IP. The ping should be successful.
3. Check if the device appears in the Licensed Devices category with Error Status "Snmp Failure". If it does, verify the following:
 - a. Verify that SNMP is enabled on your device. See [Device Prerequisite Configuration, on page 76](#) for more details.
 - b. Verify that the SNMP credentials provided on the Access Profile match the ones defined on the device.
 - c. Verify that the SNMP port 30162 is not blocked on the Windows firewall.
4. Check if the device appears in the Licensed Devices category with a partial information icon and with Error Status "Cli Failure". If it does, verify that the Telnet/SSH credentials provided in the Device Access Profile match the credentials in the device.
5. Rediscover the device after the changes have been made.

All Devices

Other device discovery can occur through Asset Discovery on the system.

1. Make sure the device IP is reachable through IND. Go to the command prompt on the windows running IND and ping the IP. The ping should be successful.
2. CIP, MODBUS, and BACnet discovery: Make sure that there is an ARP entry in the network for the CIP device.
3. PROFINET discovery: Make sure the PROFINET SNMP credentials match those in the Access Profile.
4. SNMP discovery: Make sure the SNMP credentials of the device match those in the Network SNMP Settings in the Access Profile.
5. OPC UA discovery: Make sure the OPC UA settings in the Device Access Profile match the OPC UA server configuration in the device. Only opc.tcp protocol is supported.
6. Rediscover the device after the changes have been made.

Topology Discovery

Topology is automatically triggered after an asset discovery scan (see [Topology, on page 80](#)). You can also manually trigger topology discovery on the **Operate > Topology** page to view the topology accurately after a Licensed Device Move to Licensed state.

1. If links are missing between Licensed devices, between a Licensed device and PROFINET device, or between a Licensed device and SNMP device, make sure LLDP and CDP are enabled on the device.
2. If links are missing between CIP, MODBUS, BACnet and OPC UA devices and Licensed devices, make sure there is an ARP entry in the network for the CIP, MODBUS, BACnet or OPC UA IP.

Administrative State Change Failures


Device Move to Licensed State

After you select the devices under Inventory > Licensed Devices and move the devices to the Licensed state, view the details to monitor the progress of the task. The page does not auto refresh so refresh the task detail manually every few minutes. If the task does not successfully complete, the subtask detail will provide more information regarding the failure.

Some of the common failures are:

1. The device does not have the required prerequisite configuration. See [Device Prerequisite Configuration, on page 76](#) for more details.
2. Verify that the Telnet/FTP/HTTP or SSH/SCP/HTTPS settings in the Device Access Profile match the device credentials.
3. Verify that the Windows firewall is not blocking any of the access ports specified in the Access Profile.
4. The device is not transitioned to Licensed state due to insufficient licenses. Do the following:



- a. On the **Operate > Inventory** page, click . Check the check box for License Type to display License Type in the table.
 - b. Go to **Settings > Licenses** and verify that there are enough licenses for the given license type. If not, then Import Licenses for the device type.
 - c. Try to perform the state transition again.
5. If moving devices to licensed state fails when user authentication is done through AAA servers, additional configuration is required. For example:

```
aaa new-model
!
!
aaa authentication login default group tacacs+ local
aaa authorization exec default group tacacs+ if-authenticated

tacacs-server host 10.106.224.13
tacacs-server key test123
```


On TACACS server, created authentication user name **iesadmin**, password **test123**.

On IND, created Access Profile with user name **iesadmin**, password **test123**.

CIP Backplane

Note the following when troubleshooting issues with CIP backplane discovery and CIP device state changes:



- Check the tasks (click ) for all backplane discovery operations in progress.
- The CIP device state change to licensed or device refresh operations typically take approximately 4 minutes per communication port on a licensable device for a typical /24 subnet. Therefore, depending on the number of communication modules and the subnet defined, the duration of the backplane discovery operation may vary.
- When a device refresh is triggered for backplane discovery, the slot information in that device is not refreshed.

Page Not Found

The system displays this page if you enter the wrong URL or the page does not exist.

No Permission

The system displays this page if you try to access a URL that you do not have permission to access. Permissions are mapped to the role assigned to a user by the System Administrator. Please refer to [User Roles, on page 117](#) for details on assigning permissions to users.

Configuration Archive Failures

Only one recurring configuration archive task can be created. To change the schedule, reschedule the recurring configuration archive task.

On IND restart, the Configuration Archive Service will create a recurring task if a recurring Configuration Archive was enabled earlier.

Every on-demand configuration archive task that is run is logged in **Operate > Audit Trails**. Only the scheduling of the recurring configuration archive is logged in Audit Trail.

If a configuration archive operation fails, do the following:

- Verify that the User credentials are valid for device access in the Device Access Profile for the device.
- Verify that the device is in reachable state in IND.