# Extended Enterprise Implementation Guide

## for Non-Fabric Deployment with the Cisco DNA Center

August 2019

Solution 1.0

Cisco Validated Design

**Cisco Systems, Inc.**     www.cisco.com

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

# Contents

# Extended Enterprise Implementation Guide for Non-Fabric Deployment with the Cisco DNA Center

This *Extended Enterprise Implementation Guide for Non-Fabric Deployment with Cisco DNA Center* describes the implementation of the design described in the *Extended Enterprise Design Guide*. This guide incorporates a broad set of technologies, features, and applications for helping customers extend the enterprise Information Technology (IT) services to outdoor spaces.

Cisco Validated Designs (CVDs), which provide the foundation for systems design, are based on common use cases or engineering system priorities. Each guide details the methodology for building solutions, and more importantly, the recommendations have been comprehensively tested by Cisco engineers to help ensure a faster, more reliable, and predictable deployment.

## Extended Enterprise CVD

An enterprise has production, storage, distribution, and outdoor facilities. IT reach extends beyond the traditional carpeted space to non-carpeted spaces as well. IT can now extend network connectivity, security policy, and management to the outside, warehouses, and distribution centers with the same network operating systems and network management that offer automation, policy enforcement, and assurance inside. The Cisco Digital Network Architecture (Cisco DNA) is an architecture based on automation and analytics that provides comprehensive network visibility and end-to-end policy delivery at scale. Cisco DNA enables customers to capture business intent and activate it network wide in the campus and in non-carpeted spaces where the operations happen.

The Extended Enterprise Solution CVD, which is documented in this *Extended Enterprise Implementation Guide for Non-Fabric Deployment with Cisco DNA Center*, outlines the steps for both IT and operations teams to accomplish business goals by digitizing the operations in the outdoor spaces of an enterprise. It includes guidance for implementing Extended Enterprise use cases with the customer's existing Cisco DNA Center.

## Comments and Questions

To learn more on Extended Enterprise solutions, please visit:

- https://www.cisco.com/go/extendedenterprise
- https://www.cisco.com/go/iotcvd

## Scope and Audience for this Document

This implementation guide provides deployment guidance for an Extended Enterprise network design. It is a companion to the associated design and deployment guides for enterprise networks, which provide configurations explaining how to deploy the most common implementations of the designs as described in this guide. It discusses the Extended Enterprise implementation for non-fabric technology with the Cisco DNA Center.

**Cisco Systems, Inc.** www.cisco.com

For the associated deployment guides, design guides, and white papers, see refer to the following URLs:

- Cisco Enterprise Networking design guides:
  - https://www.cisco.com/go/designzone
- Cisco IoT Solutions design guides:
  - https://www.cisco.com/go/iotcvd
- Cisco Extended Enterprise Solutions overview:
  - https://www.cisco.com/go/extendedenterprise
- Extended Enterprise Design Guide:
  - https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/EE/DG/ee-dg.html

## What is in this Guide?

This document is organized in the following sections:

| | |
|---|---|
| Implementation Overview, page 3 | Discusses overall network topology and considerations. |
| Design, page 6 | Details Cisco DNA Center design options relevant to Extended Enterprise implementation for non-fabric technology. |
| Provisioning, page 12 | Provides guidance to add Industrial Ethernet (IE) switches to the network and provision non-fabric wireless, perform software upgrades, and add endpoints to the network. |
| Security, page 27 | Explains how to add security policies and necessary configurations to provide micro segmentation and endpoint visibility. |
| Assurance, page 43 | Gives an overview of Cisco DNA Center assurance capabilities for Extended Enterprise deployments. |
| Appendix A: Installation and Setup, page 50 | Installation and setup references. |
| Appendix B: Sample Template used in CVD Verification, page 50 | Sample templates for device sensor configuration, authentication policies, onboarding configuration, and interface configurations. |

This guide assumes that the user has already installed Cisco DNA Center, Cisco Identity Services Engine (ISE), and the Wireless LAN Controller (WLC) in the enterprise network. For more details, refer to the *Cisco Software-Defined Access Deployment Guide* at the following URL:

- https://cvddocs.com/fw/251-prime

# Implementation Overview

The Extended Enterprise Non-Fabric architecture managed by Cisco DNA Center is similar to the architecture described in the Cisco Enterprise Network and Campus Wired and Wireless LAN CVDs. The design enables wired and wireless communications between devices in an outdoor or a group of outdoor environments, as well as interconnection to the WAN and Internet edge at the network core.

### References

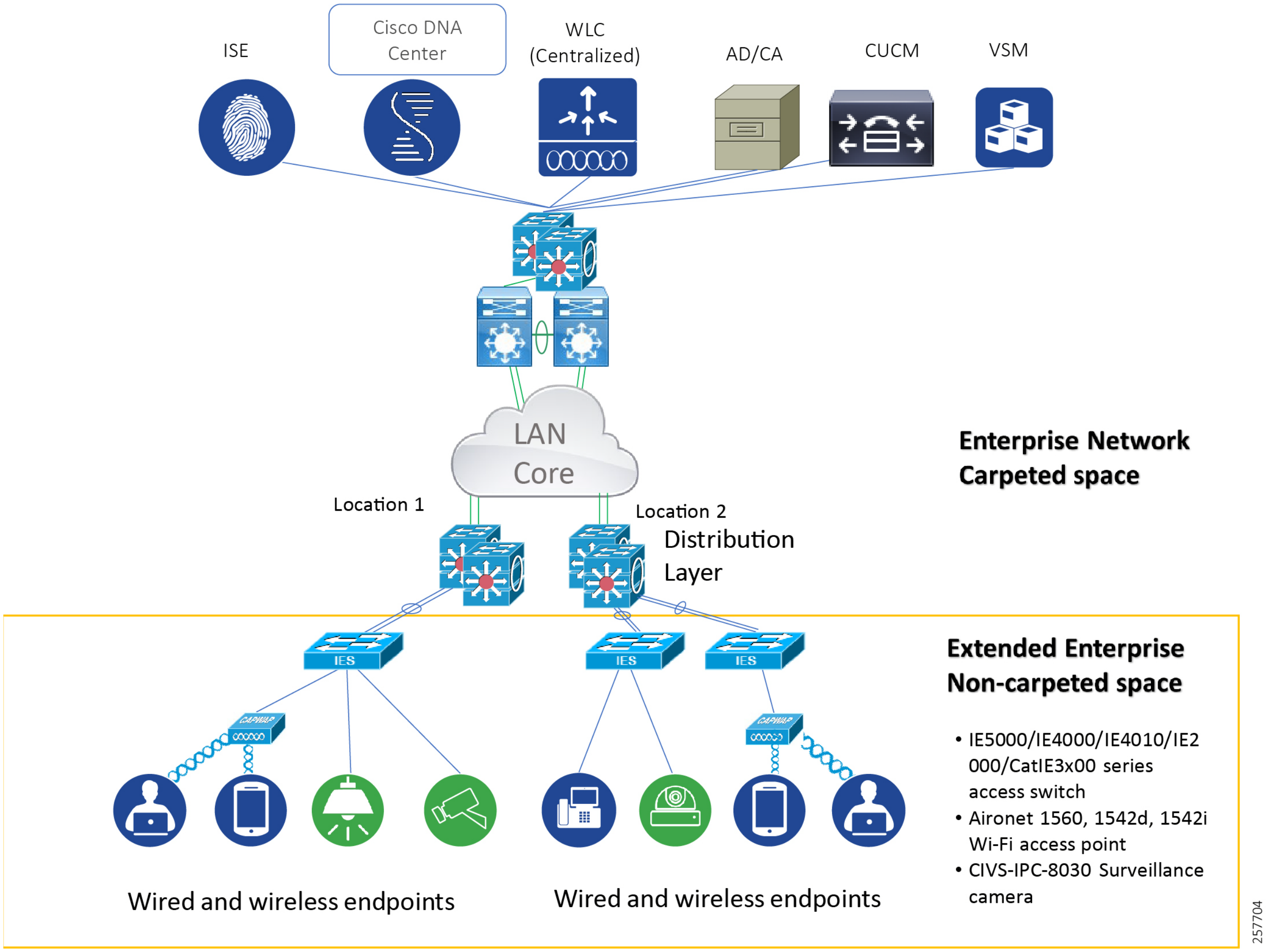
- Cisco Enterprise Network Design Guide:
  - https://www.cisco.com/c/en/us/solutions/design-zone/networking-design-guides/digital-network-architecture-design-guides.html
- Campus Wired and Wireless LAN website:
  - https://www.cisco.com/c/en/us/solutions/design-zone/networking-design-guides/campus-wired-wireless.html

Each building floor or geographic location will have an enterprise access switch (for example, the Cisco Catalyst 9300) with at least two arranged in a stack. Ruggedized IE switches are connected to the enterprise access switches and thus extend the enterprise network to the non-carpeted spaces. The Extended Enterprise region allows both wired and wireless connectivity, and a centrally-located WLC connects the non-fabric access point (AP) to the enterprise and Extended Enterprise. For network latency requirements from the AP to the WLC, and from the Cisco DNA Center to a fabric edge, refer to the *Cisco DNA Center User Guide* at the following URL:

- https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-user-guide-list.html

Industrial switches are connected in a star topology with redundant links aggregated in an EtherChannel. Figure 1shows the validation topology.

**Figure 1 Validation Topology**


ISE
Cisco DNA Center
WLC (Centralized)
AD/CA
CUCM
VSM
LAN Core
Location 1
Location 2
Distribution Layer
Enterprise Network
Carpeted space
IES
CAPWAP
Wired and wireless endpoints
Wired and wireless endpoints
Extended Enterprise
Non-carpeted space
• IE5000/IE4000/IE4010/IE2000/CatIE3x00 series access switch
• Aironet 1560, 1542d, 1542i Wi-Fi access point
• CIVS-IPC-8030 Surveillance camera
257704

Security policies are uniformly applied, which provides consistent treatment for a given service across the Enterprise and Extended Enterprise networks. Controlled access is given to shared services and other internal networks by appropriate authorization profile assignments.

## Validated Hardware/Software Matrix

Table 1 contains a list of the verified hardware and software components.

**Table 1 Verified Hardware and Software Components**

| Role | Cisco Platforms | Version | Description | CVD Verified |
|---|---|---|---|---|
| Extended Enterprise Access Layer | IE2000 series | IOS 15.2.6E2a | Industrial Ethernet Switches | Yes |
| | Cisco Catalyst IE3200 / Cisco Catalyst IE3300 series | IOS XE 16.11.1a | Ruggedized full Gigabit Ethernet with a modular, expandable up to 26 ports. Up to 16 PoE/PoE+ ports. | Yes |
| | IE4000 series | IOS 15.2.6E2a | Ruggedized DIN rail-mounted 40 GB Ethernet switch platform. IE4010 Series Switches with 28 GE interfaces and up to 24 PoE/PoE+ enabled ports. | Yes |
| | IE5000 series | IOS 15.2.6E2a | Ruggedized One RU multi-10 GB aggregation switch with 24 Gigabit Ethernet ports plus 4 10-Gigabit ideal for the aggregation and/or backbones, 12 PoE/PoE+ enabled ports. | Yes |
| Non-fabric AP | AP1560 | AireOS 8.8.100.0 | Rugged outdoor 802.11ac Wave 2 AP, supports up to 1.3-Gbps data rates with 3 x 3 MIMO | -- |
| Enterprise Access Layer | Cat 9300 | IOS-XE 16.6.5 | 480 Gbps stacking bandwidth. Sub-50-ms resiliency. UPOE and PoE+. 24-48 multigigabit copper ports. Up to 8 port fiber uplink. AC environment. | -- |
| Cisco DNA Center Appliance | DN2-HW-APL | Not applicable | U - 44 core, L - 56 core<br>2x Two 10 Gbps Ethernet ports, One 1 Gbps management port | -- |
| Cisco DNA Center | -- | 1.2.10 | Single Pane of Glass | -- |
| Cisco Identity Services Engine (ISE) | Cisco SNS-3515 and SNS-3595 Secure Network Server | ISE 2.4 Patch 5 | Policy Engine | -- |
| Wireless Controller | Cisco WLC 3504 | AireOS 8.8.100.0 | Wireless Controller | Yes |

**Tip:** The Cisco Industrial Wireless 3700 Series will be supported by Cisco DNA Center in an upcoming road map.

# Design

The Cisco DNA Center Network configuration tab on the user interface has a design section to create the structure and framework of your network, including the physical topology, network settings, and device type profiles that you can apply to devices. As part of this design, the following sections describe functionality:

- Designing Network Hierarchy and Settings, page 6
- Configuring Global Wireless Settings for Non-Fabric Deployment, page 6
- Creating SSIDs for a Guest Wireless Network, page 7
- Managing the Image Repository, page 8

## Designing Network Hierarchy and Settings

The network hierarchy represents your network's geographical locations. It contains sites, which, in turn, contain buildings and areas. You can create site and building IDs to easily identify where to apply design settings or configurations later. By default, one site is called **Global**.

This guide assumes that the administrator has already configured network sites, network services for sites, and credentials for discovery and management as described in the *CVD Software-Defined Access Deployment Guide*, which can be found at the following URL:

- https://cvddocs.com/fw/251-prime

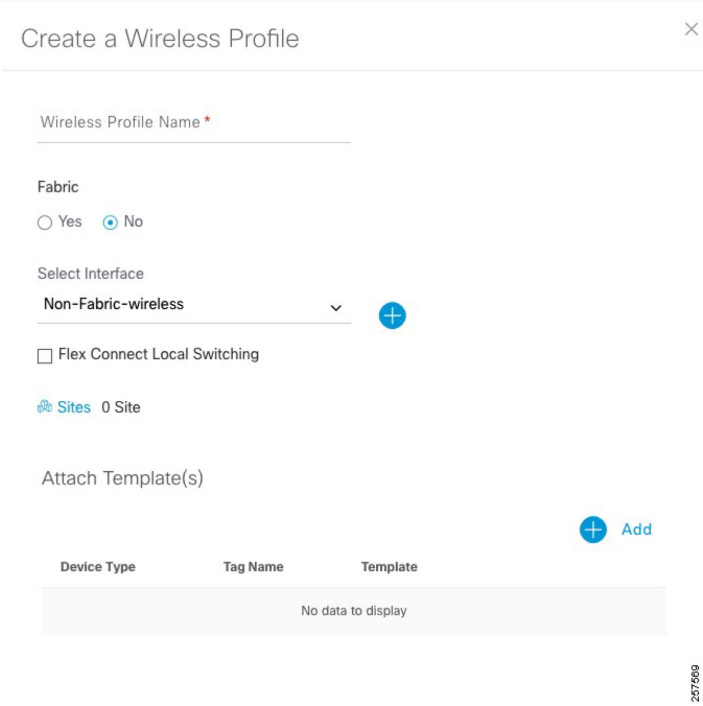
Note that IP address pool configuration is not needed in the non-fabric deployment.

## Configuring Global Wireless Settings for Non-Fabric Deployment

Global wireless network settings include settings for Service Set Identifier (SSID), wireless interfaces, wireless radio frequency (RF), and sensors. The following section provides steps for creating SSIDs.

1. From the **Cisco DNA Center dashboard,** navigate to **DESIGN > Network Settings > Wireless**. In the **Enterprise Wireless** section, click **+ Add** and in the **Create an Enterprise Wireless Network** wizard, supply the following information:
   - Enter the **Wireless Network Name (SSID)**.
   - Under **TYPE OF ENTERPRISE NETWORK**, select **Voice and Data**.
   - For the **WIRELESS OPTION**, click the radio button of the appropriate frequency.
   - Fort **LEVEL OF SECURITY**, select **WPA2 Enterprise**.
     - (Optional) De-select **BROADCAST SSID** if you do not want the SSID to be visible.
     - Under **ADVANCED SECURITY OPTIONS**, select **Adaptive**.
2. Click **Next** to continue in the wizard and supply the following information:
   - Enter a **Wireless Profile Name**.
   - Under **Fabric**, select **No**.
   - Under **Select Interface**, choose an interface name from the drop-down list or click **+** to create a new wireless interface. This is the VLAN ID that is associated with the wireless interface.
   - Under **Sites**, select the location where the SSID will broadcast and include floors to include in SSID coverage.

**Figure 2 Creating a Wireless Profile**



Create a Wireless Profile

Wireless Profile Name *

Fabric

○ Yes ● No

Select Interface

Non-Fabric-wireless

□ Flex Connect Local Switching

Sites 0 Site

Attach Template(s)

| Device Type | Tag Name | Template |
|---|---|---|
| No data to display | | |

3. Click **Add** to create the wireless profile and associate it with a site. Then click **Finish** to continue. The **DESIGN > Network Settings > Wireless** screen displays.

Repeat this procedure for additional SSIDs, using the same network profile and any new location profiles to be associated with an SSID.

## Creating SSIDs for a Guest Wireless Network

Follow these steps to design a fabric guest wireless SSID:

1. From **DESIGN > Network Settings > Wireless**, click **+ Add** in the **Guest Wireless** section. Next, in the **Create a Guest Wireless Network** wizard, supply the following information:

   – Enter the **Wireless Network Name (SSID)** (example: **Guest**).

   – Under **LEVEL OF SECURITY**, select **Web Auth**.

   – Under **AUTHENTICATION SERVER**, select **ISE Authentication**.

   Retain the other default selections and click **Next** to continue in the wizard.

2. In the **Wireless Profiles** section, select the Profile Name corresponding to the deployment location. In the slide-out panel, choose **Yes** for **Fabric** and retain the other default information. At the bottom of the panel, click **Save**, and then click **Next**.

3. In the **Portals** screen, click **+ Add**. The **Portal Builder** screen displays.

4. Supply a name for the **Guest Portal**, make any desired customizations, and then at the bottom of the screen, click **Save**. A guest web authentication portal is generated for the site, and you are returned to the previous screen.

5. Click **Finish**. The wireless LAN design is created and is ready to deploy.

# Managing the Image Repository

The Cisco DNA Center stores all the unique software images according to image type and version. You can view, import, and delete software images.

## Viewing Software Images

1. From the Cisco DNA Center dashboard, choose **Design > Image Repository**.

   You can also access the image repository via **Tools > Image Repository**. Software images are displayed by device type. Virtual devices are not displayed by default.

2. Toggle the **Virtual** tab to view images for virtual devices.

   As devices are discovered or manually added to the Cisco DNA Center, information about their software image is added to the image repository. During discovery:

   - If an image for a device does not appear under its family, the Cisco DNA Center will add an entry for that image under the correct platform.

   - If the image is already listed for that device family, the **Using Image** column will be incremented for the appropriate family.

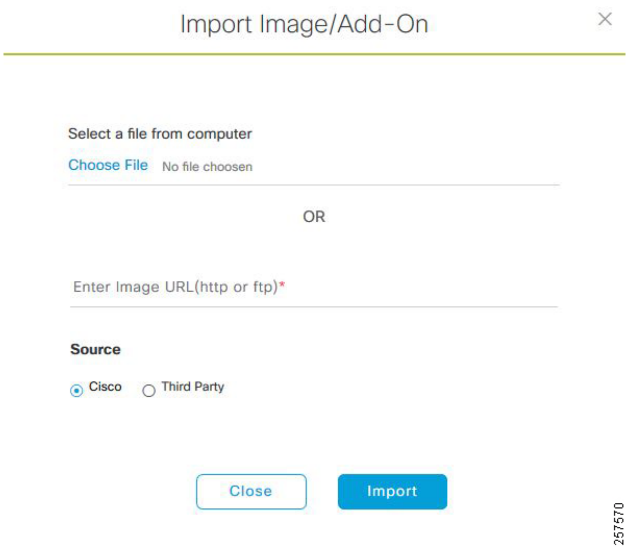
## Uploading an Image

1. From the **Cisco DNA Center** dashboard, choose **Design > Image Repository**.

2. Click **+ Import**.

3. In the pop-up window, click **Choose File** to navigate to a software image stored locally on your PC or specify an HTTP or FTP source where the image resides. For Cisco software images, ensure that the **Cisco** radio button beneath **Source** is selected. When finished, click **Import** at the bottom of the pop-up window.

**Figure 3 Importing Image**



Import Image/Add-On

Select a file from computer

Choose File No file choosen

OR

Enter Image URL(http or ftp)*

Source

● Cisco ○ Third Party

4. Verify that the image was imported correctly. After successful import of an image, a notification is displayed at the bottom right of the screen. If an image is not imported directly from Cisco.com, the user will need to navigate to the **Imported Images** group and click the drop-down arrow to display all imported images.

   **Tip:** If the image you just imported is not present in the list of imported images, click **Refresh** next to the **Filter** icon. The total number of images will increment by one and the image will be displayed in the list of imported images.

**Tip:** If the trash can icon to the far right of an image is blue, the image has been imported to the Cisco DNA Center. If the trash can icon is gray and not selectable, the image has not been imported to the Cisco DNA Center.

5. Assign the appropriate image to a platform by clicking **Assign** next to the image. A pop-up window will appear, on which the user can select device platforms for the image. When finished selecting platforms, click **Assign**.

## Network Profiles for Switching

During device provisioning, network profiles are used to assign configuration templates to devices based on their device family and site. Before creating a network profile, templates must be created in the Template Editor. For devices that require a similar configuration, a template helps to reduce the configuration time by using variables and logic statements as placeholders for any unique settings.

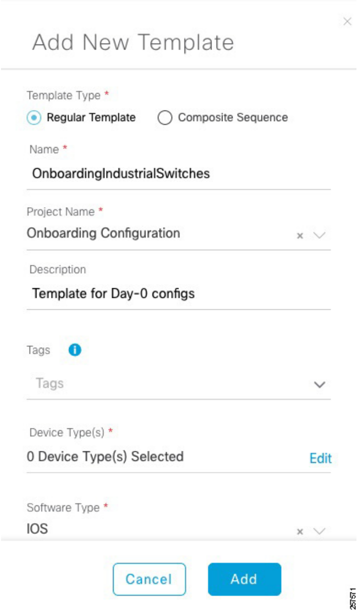
In order to configure a new device with more specific configuration during the PNP process, a template must be created. Day-0 configuration templates, also called Onboarding templates, must be created with the configuration to be applied to the new device. Day-N templates are used to push the configuration to devices already in Cisco DNA Center inventory.

Templates are logically grouped into projects. The Cisco DNA Center has a default project for the Day-0 configuration, but if you are creating Day-N templates, you may need to create additional projects. The following section explains template and project creation.

### Creating the Onboarding Template (Day-0)

1. From the **Cisco DNA Center** dashboard, choose **Tools > Template Editor**.
2. Onboarding templates are added under **Onboarding Configuration**. Click **+** and select **Create Template**.
3. In the **Add New Template** window, click **Regular Template**.
4. Enter a name for the template.
5. In the **Project Name** drop-down list, select **Onboarding Configuration**. A tag can be assigned to the template so that it will only be available to devices in inventory with a matching tag. In the **Device Type** field, click **Edit** to select device platforms for this template.

**Figure 4 Adding Template**



Add New Template

Template Type *

● Regular Template ○ Composite Sequence

Name *

OnboardingIndustrialSwitches

Project Name *

Onboarding Configuration

Description

Template for Day-0 configs

Tags

Tags

Device Type(s) *

0 Device Type(s) Selected

Software Type *

IOS

6. In the **Select Device Type(s)** window, drill down to platforms or grouping of platforms.

   – If all selections below a parent grouping are selected, a blue check is displayed in the check box.

   – If some, but not all selections below a parent grouping are selected, a blue square is displayed.

   Select all device platforms or groupings of platforms a template should apply to and click **Back to Add New Template** to return to the **Add New Template** window.

7. Under **Software Type**, select the software type for the template. Any template assigned to IOS software will also be available to IOS-XE and IOS-XR software devices, but templates made for IOS-XE and IOS-XR software will not be available to other IOS software devices. Once complete, click **Add**.

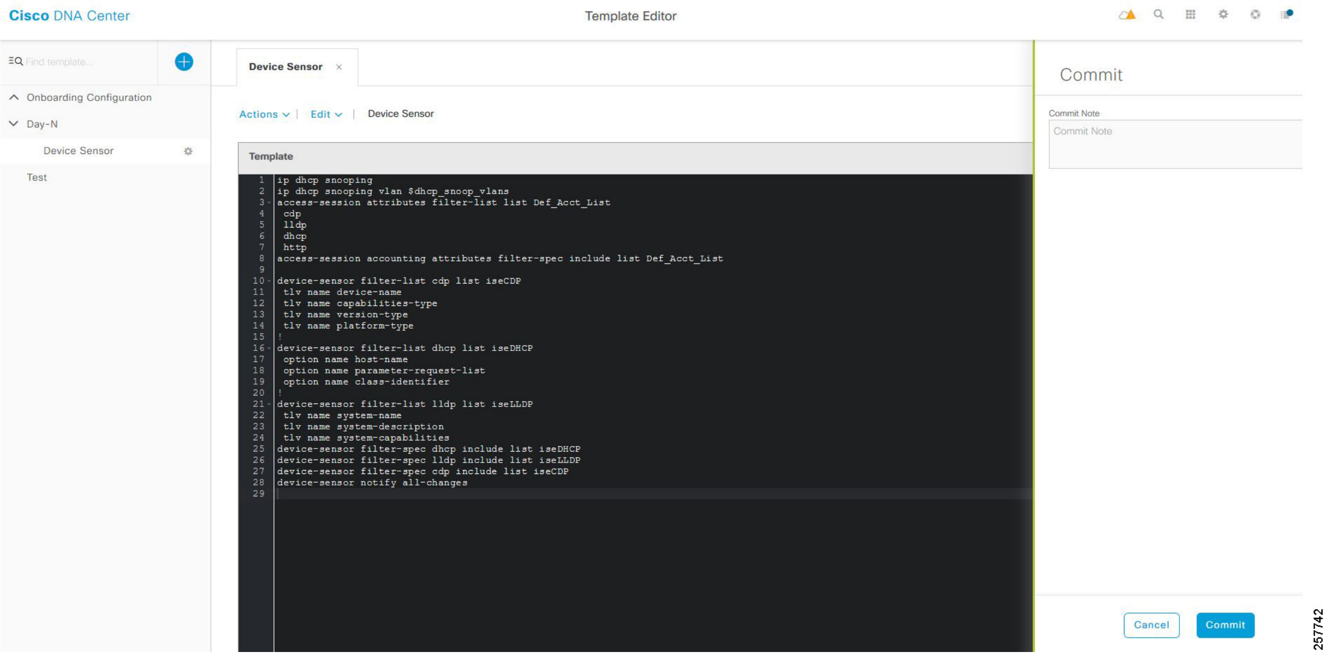
8. After the template is created, click the template name in the left window to edit. In the **Template Editor** window, enter any content for the template. The Cisco DNA Center uses the Velocity Templating Language (VTL) to allow the use of variables and logic statements to generate a configuration from a template. Appendix B: Sample Template used in CVD Verification, page 50 includes some template examples.

   **Note:** In the Cisco DNA Center, configuration for devices is rendered via VTL. Velocity is a template programming language. The generated configuration can be used for either Plug and Play (Day-0) or Provisioning (Day-N) workflows. In the Template Editor, configuration templates can be created using variables, macros, and loops that are then interpreted by Velocity to produce device configuration. All configurations are rendered on the Cisco DNA Center, and VTL does not have access to the current running configuration of the device.

9. Click **Actions** and then click **Save**. The Cisco DNA Center will check for VTL syntax errors in the template. If errors exist, the template will not be saved.

10. For the latest version of a template to be available in **Design > Network Profiles**, the template must be committed. Click **Actions** and then click **Commit**. In the **Commit** window, click **Commit**.

**Figure 5 Committing Template**



```
ip dhcp snooping
ip dhcp snooping vlan $dhcp_snoop_vlans
access-session attributes filter-list list Def_Acct_List
 cdp
 lldp
 dhcp
 http
access-session accounting attributes filter-spec include list Def_Acct_List

device-sensor filter-list cdp list iseCDP
 tlv name device-name
 tlv name capabilities-type
 tlv name version-type
 tlv name platform-type
!
device-sensor filter-list dhcp list iseDHCP
 option name host-name
 option name parameter-request-list
 option name class-identifier
!
device-sensor filter-list lldp list iseLLDP
 tlv name system-name
 tlv name system-description
 tlv name system-capabilities
device-sensor filter-spec dhcp include list iseDHCP
device-sensor filter-spec lldp include list iseLLDP
device-sensor filter-spec cdp include list iseCDP
device-sensor notify all-changes
```

## Creating Day-N Template (Optional)

Projects are logically grouped templates. Creating a Day-N template follows the same procedure as above, but instead of selecting **Onboarding Configuration** in the **Project Name** drop-down list, create a new project. Unlike templates grouped in the Onboarding Configuration project that are only available during the Plug and Play process, Day-N templates are available for use during provisioning of a device in the Cisco DNA Center inventory.

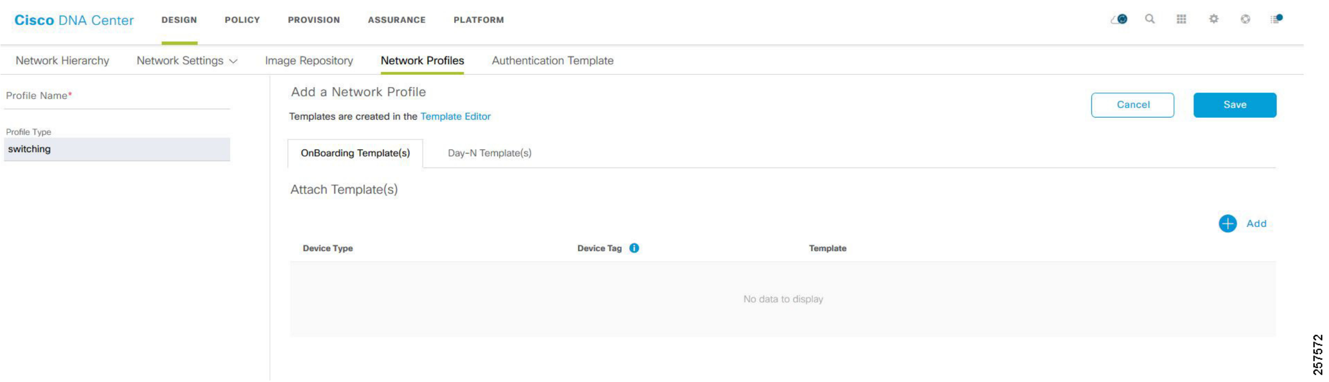
1. To create a new project, click **+** and then select **Create Project**.
2. In the **Add New Project** window, enter a unique name for the project and then click **Add**. The new project will appear in the left window.
3. When creating a Day-N template, select the appropriate project.

## Creating a Network Profile

Before a device can be provisioned using a template, it must be associated with a network profile and the profile must be assigned to a site.

1. Navigate to **Design > Network Profiles**. Click **Add Profile**.
2. Select **Switching** to create a switching network profile.
3. Enter a unique Profile Name. Select **OnBoarding Template(s)** or **Day-N Template(s)** based on where the appropriate template is grouped.

**Figure 6 Creating a Network Profile**



Profile Name*

Profile Type
switching

4. To associate a template to the network profile, click **+Add**.

5. Under the **Device Type** column, drill down to a specific platform or group of devices. Only one platform type or one parent group of devices may be selected per field.

6. Under the **Template** column, select the appropriate template.

7. (Optional) Click **+Add** to create another device type to template association within one network profile if needed.

8. Click **Save**.

   **Tip:** If the expected template does not appear after selecting **Device Typ**e or **Device Role**, navigate back to **Template Editor** and ensure that the correct **Device Type** and **Role** have been added to the template. If changes have been made to the template and it still does not appear as a selection in **Design > Network Profiles**, ensure that the changes have been saved and committed.

## Associating Network Profile to a Site

Once the network profile has been created and has templates associated, it must be assigned to a site. On the **Network Profiles** page, click **Assign Site**. Click a site or sites where the network profile should be assigned. If a network profile is assigned to a site, any device provisioned at the site with a device type and role that matches a template association within the profile will have a template available during the provisioning step.

# Provisioning

## Provisioning IE Switches using Plug and Play

Cisco Plug and Play (PnP) provides a highly secure, scalable, seamless, and unified ZTD experience. Cisco industrial switches that are running IOS or IOS-XE software have a PnP agent embedded in the software that communicates with the PnP deployment server. The PnP agent runs on a device if no startup configuration exists, such as when a device is powered on for the first time or is reset to factory defaults. The PnP agent attempts to discover the PnP deployment server via DHCP or Domain Name System (DNS). The Cisco DNA Center serves as the PnP server for the Extended Enterprise deployment.

### PnP Requirements for DHCP Discovery

- DHCP server with option 43 configured pointing to the Cisco DNA Center IP.
- DHCP server must accept the Cisco vendor-specific option 60 case sensitive value *ciscopnp*.
- The IP helper address should be configured on a Layer 3 interface of the distribution switch.

### Example of DHCP Configuration

DHCP option 43 consists of a string value that is configured as follows on a Cisco router CLI that is acting as a DHCP server:

```
ip dhcp pool pnp_device_pool          <-- Name of DHCP pool
network 192.168.1.0 255.255.255.0     <-- Range of IP addresses assigned to clients
default-router 192.168.1.1            <-- Gateway address
option 43 ascii "5A1N;B2;K4;I172.19.45.222;J80"     <-- Option 43 string
```

The option 43 string has the following components, delimited by semi-colons:

- **5A1N;**—Specifies the DHCP sub-option for PnP, active operation, version 1, no debug information. It is not necessary to change this part of the string.
- **B2;**—IP address type, B2 stands for IPv4, B1 should be used for hostname.
- **Ixxx.xxx.xxx.xxx;**—IP address or hostname of the Cisco DNA Center controller (following a capital letter i). In this example, the IP address is 172.19.45.222.
- **Jxxxx**—Port number to use to connect to the Cisco DNA Center controller. In this example, the port number is 80. The default is port 80 for HTTP and port 443 for HTTPS.
- **K4;**—Transport protocol to be used between the device and the controller, use K4 for HTTP (default) or K5 for HTTPS.

For more information, refer to the *Cisco Digital Network Architecture Center User Guide*.

## PnP Requirements for DNS Discovery

- Domain name option configured on DHCP server
- DNS server option configured on DHCP server
- PnP server (Cisco DNA Center) resolves to PnP deployment server IP in DNS
- IP helper address should be configured on distribution switch

## Configuration on Distribution Switch to Support PnP

1. PnP supports use of VLAN 1 by default for PnP. To use a VLAN other than 1, the adjacent upstream device from the PnP device must have **pnp startup VLAN** *vlan* configured globally with the VLAN used for PnP. This will create the VLAN on the PnP device for use in the PnP provisioning process. Enter the following configuration line:

```
switch(config)#pnp startup VLAN 80
```

2. PnP can operate with a single trunk link between the PnP switch and the upstream device, but it is highly recommended to use an EtherChannel for high availability. This guide assumes the use of EtherChannel in the sample configuration. The **no port-channel standalone-disable** command is required on the upstream switch to prevent the port channel from being disabled since it is not configured on the PnP switch at boot time.

```
switch(config)#interface Port-channel20
switchport mode dynamic desirable
no port-channel standalone-disable
```

3. (Optional) If the native VLAN in the trunk will be different than 1, add the following line to the configuration:

```
switch(config)# interface Port-channel20
switchport trunk native vlan 900
```

4. Add VLANs to the trunk, making sure to include native VLAN, PnP VLAN, and any VLAN that is intended to be trunked to the switch.

```
switch(config)# interface Port-channel20
switchport trunk allowed vlan 80-85,900
```

The following are examples of EtherChannel configuration; the first example has a non-default native VLAN and the second example shows a configuration with native VLAN 1:

### Configuration Example for Non-Default Native VLAN

```
interface Port-channel20
switchport trunk native vlan 999
switchport trunk allowed vlan 80-85,999
switchport mode dynamic desirable
no port-channel standalone-disable
!
interface GigabitEthernet1/0/7
description EE-port
switchport trunk native vlan 900
switchport trunk allowed vlan 80-85,900
switchport mode dynamic desirable
channel-protocol lacp
channel-group 20 mode passive

interface GigabitEthernet2/0/7
description EE-port
switchport trunk native vlan 900
switchport trunk allowed vlan 80-85,900
switchport mode dynamic desirable
channel-protocol lacp
channel-group 20 mode passive
```

### Configuration Example for Native VLAN 1

```
interface Port-channel21
switchport trunk allowed vlan 1,80-85
switchport mode dynamic desirable
no port-channel standalone-disable

interface GigabitEthernet1/0/8
description EE-port
switchport trunk allowed vlan 1,80-85
switchport mode dynamic desirable
channel-protocol lacp
channel-group 21 mode passive

interface GigabitEthernet2/0/8
description EE-port
switchport trunk allowed vlan 1,80-85
switchport mode dynamic desirable
channel-protocol lacp
channel-group 21 mode passive
```

## Planned Provisioning

Planned provisioning requires anticipation of new PnP-capable devices connecting to the network. To prepare for planned provisioning of a device, an administrator should:

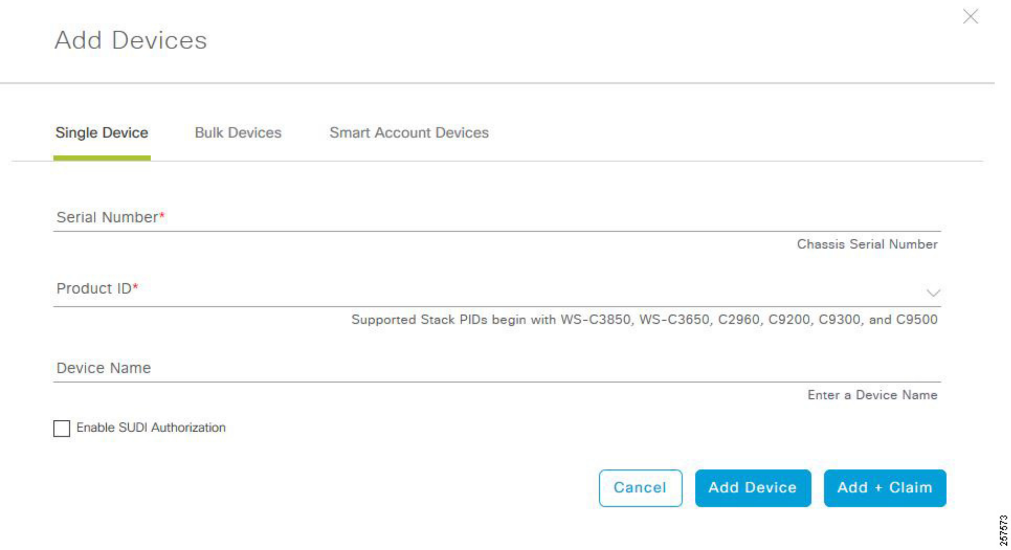
- (Optional) Upload software images to deploy to devices.
- Create configuration templates.
- Add the device to DNA manually, by comma-separated values (CSV) file, or by a linked Cisco Smart Account.

- Assign a provisioning task to the device by claiming the device.

  **Warning:** Devices that boot up and contact the Cisco DNA Center will be automatically provisioned if they have been claimed. If not, the devices will remain in a planned state until the administrator claims them.

1. To add a new PnP device to the Cisco DNA Center, navigate to **Provision > Devices > Plug and Play**.
2. Click **Add**. The **Add Devices** window displays.

**Figure 7 Adding Devices for Planned Provisioning**



3. Select **Single Device** to add one device at a time, **Bulk Devices** to add multiple devices via a CSV file, or **Smart Account Devices** to add devices from a linked Smart Account.
4. For a single device, enter the device serial number and product ID. A device name is not required and if one is not entered, the displayed device name on the **Plug and Play Devices** page will be the serial number of the device.
5. (Optional) You can enable secure device authentication and communication using secure unique device identifiers (SUDI). Click the check box next to **Enable SUDI Authentication**.

   **Warning:** SUDI Authentication is not supported on IE2000, IE4000, or IE5000 IOS 15.2.6E2a. As an alternative, skip Step 5.
6. Click **Add + Claim** to add the device and continue to claim the device as detailed in the section Claiming a Device, page 16.

   Note that selecting the **Add Device** option will add the device to the **Plug and Play Devices** page without claiming it. If that is the case, the device can be claimed later by either clicking the check box next to the device name and then clicking **Actions > Claim**, or by clicking the device name and then clicking **Claim** in the pop-up window.

## Unclaimed Provisioning

If a PnP-capable device is connected to the network, and boots with no startup configuration, it will attempt to contact the PnP deployment server. If an administrator has not previously added this device to the Cisco DNA Center, the Cisco DNA Center will use information from the PnP discovery process to add the device to the **Plug and Play Devices** page. An entry will be created with serial number as the Device Name. The Serial Number and Product ID fields will be pre-filled. Since no details about the device were entered previously, the device is in an unclaimed state. It will remain in this state until it is claimed.

A device in the unclaimed state can be claimed by the following:

1. To add a new PnP device to Cisco DNA Center, navigate to **Provision > Devices > Plug and Play**.
2. Click the check box next to the device name and then click **Actions > Claim** or click the device name and then click **Claim** on the pop-up window.

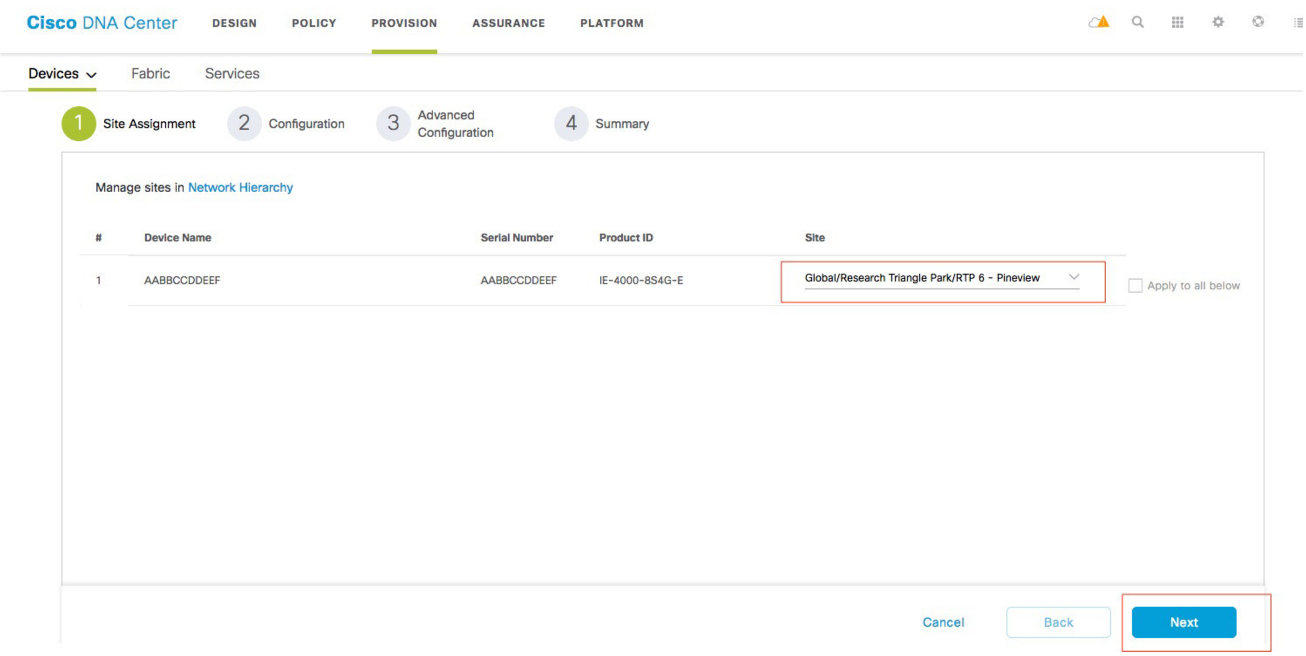
## Claiming a Device

Claiming a device provisions it by assigning it to a site, deploying settings, and adding it to inventory. Once a device has been added to Cisco DNA Center by an administrator as a planned device or added to Cisco DNA Center by contacting the PnP deployment server as an unclaimed device, it will appear on the **Plug and Play Devices** page, but it will not appear on the **Inventory** page until it has been successfully claimed.

If not done before, begin assigning a provisioning workflow by clicking the check box next to one or multiple devices. Multiple devices may be claimed at the same time. Then click **Actions > Claim**.

1. Assign a device to a site. In the drop-down list under the **Site** column, select the site where the device resides. This will determine what network settings the device will receive based on the site-level settings set in **Design > Network Settings**. Click **Next** to continue.

**Figure 8 Device Site Assignment**



Manage sites in Network Hierarchy

| # | Device Name | Serial Number | Product ID | Site |
|---|---|---|---|---|
| 1 | AABBCCDDEEF | AABBCCDDEEF | IE-4000-8S4G-E | Global/Research Triangle Park/RTP 6 - Pineview |

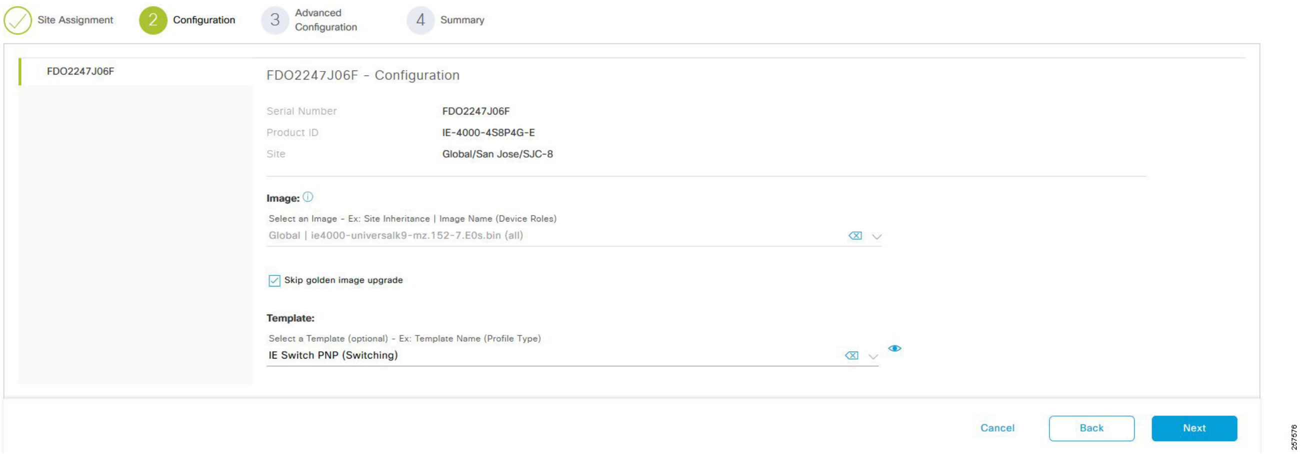
□ Apply to all below

2. For the **Configuration** step, options exist to upgrade the golden image. A golden image is required to upgrade a device in Cisco DNA Center. The golden image for a device family is set in **Design > Image Repository**.
   - If a golden image is not set for the device family prior to claiming, upgrading the image is not available.
   - If a golden image is set for a device family, but you do not want to upgrade, click the check box next to **Skip Golden Image Upgrade**.

   **Warning:** Golden Image Upgrade is not supported on Cisco DNA Center 1.2.10 for IE switches; as an alternative, skip this option and upgrade later following the steps in Provisioning a Software Image, page 24.

3. An option also exists to apply a template to a device. If a template in the Template Editor matches both the device family and device role, it will be selectable in the drop-down list. Make selections for image upgrade and template for all devices being claimed and then click **Next**.

## Figure 9 Plug and Play Device Configuration



FDO2247J06F - Configuration

Serial Number FDO2247J06F
Product ID IE-4000-4S8P4G-E
Site Global/San Jose/SJC-8

Image:
Select an Image - Ex: Site Inheritance | Image Name (Device Roles)
Global | ie4000-universalk9-mz.152-7.E0s.bin (all)

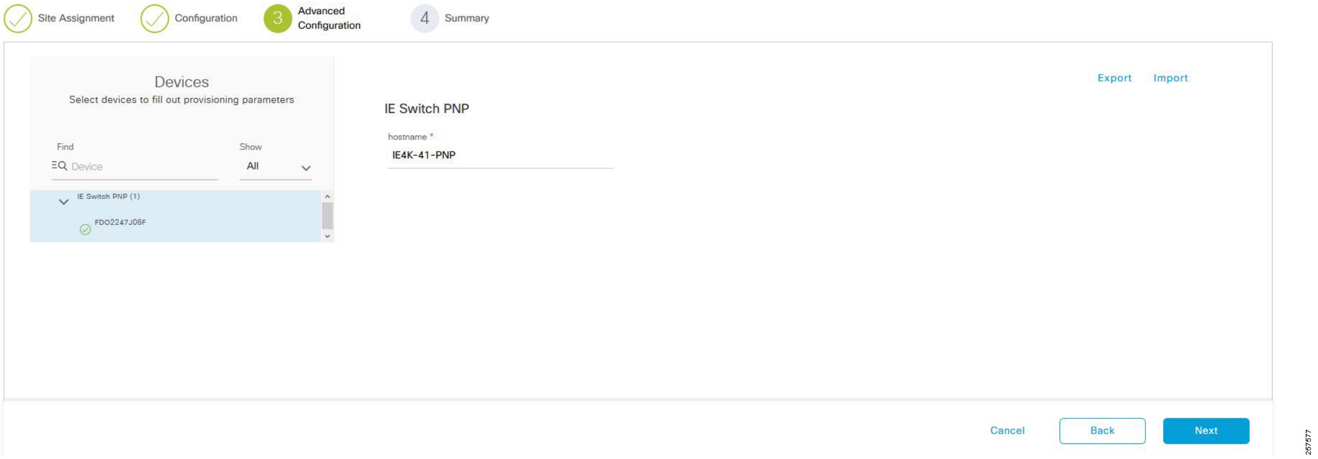
☑ Skip golden image upgrade

Template:
Select a Template (optional) - Ex: Template Name (Profile Type)
IE Switch PNP (Switching)

4. For the **Advanced Configuration** step, all variables found in templates from the previous step are displayed. Select each device being claimed and enter values for any variables. All required variables for each device must contain values before clicking **Next**.

   If no templates were selected during the Configuration step or the templates do not contain variables, click **Next** to bypass the **Advanced Configuration** step.

## Figure 10 Plug and Play Advanced Configuration



Devices
Select devices to fill out provisioning parameters

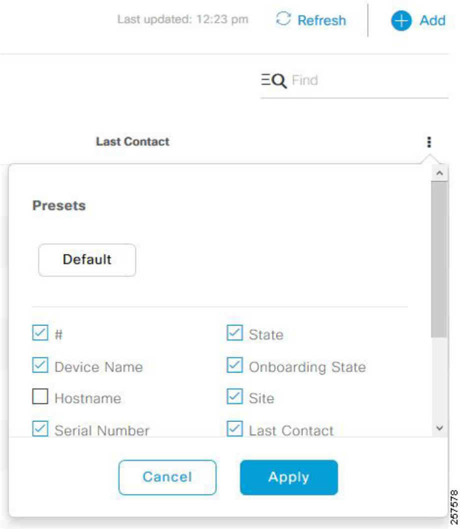
IE Switch PNP
hostname *
IE4K-41-PNP

5. For the **Summary** step, click the drop-down arrows next to **Device Details**, **Image Details**, **Day-0 Configuration Preview**, and **Template CLI Preview** to review details.
6. When you have finished reviewing, click **Save**.
7. On the **Information** pop-up window, click **Yes** to claim the devices.

After clicking **Yes** to claim devices, the Cisco DNA Center will begin provisioning any devices, claimed or unclaimed, that have previously contacted the Cisco DNA Center. If a device is unclaimed, it will briefly move into the planned state before the execution begins. If a device is in the planned state, but has not yet contacted the Cisco DNA Center, execution will begin automatically when the device successfully contacts the Cisco DNA Center.

**Tip:** When onboarding devices with PnP, it is highly recommended to add the **Onboarding State** column to the table on the **Plug and Play Devices** page. This gives a much more granular view into a device's onboarding status than the **State** field. Click **+Add** on the far right of the header row to add or remove columns.

**Figure 11 Adding Columns to Plug and Play View**



☑ #
☑ Device Name
□ Hostname
☑ Serial Number
☑ State
☑ Onboarding State
☑ Site
☑ Last Contact

After successful claiming, the status of the device in the PnP window will be provisioned. The device will be added to the Cisco DNA Center inventory located at **Provision > Devices > Inventory**. Once in inventory, a device discovered and provisioned via PnP may require further provisioning using Day-N templates.

## Plug and Play Troubleshooting

The following is an output of a successful PnP process. If the process fails on the switch, read this section for troubleshooting tips.

```
May  2 14:47:40.877: %PNPA-DHCP Op-43 Msg: Process state = READY
May  2 14:47:40.877: %PNPA-DHCP Op-43 Msg: OK to process message
May  2 14:47:40.880: XML-UPDOWN: PNPA_DHCP_OP43 XML Interface(102) UP. PID=470
May  2 14:47:40.880: %PNPA-DHCP Op-43 Msg: _pdoon.1.ntf.don=470
May  2 14:47:40.880: %PNPA-DHCP Op-43 Msg: _pdoop.1.org=[A1D;B2;K4;I10.1.3.73;J80]
May  2 14:47:40.880: %PNPA-DHCP Op-43 Msg: _pdgfa.1.inp=[B2;K4;I10.1.3.73;J80]
May  2 14:47:40.880: %PNPA-DHCP Op-43 Msg: _pdgfa.1.B2.s12=[ ipv4 ]
May  2 14:47:40.880: %PNPA-DHCP Op-43 Msg: _pdgfa.1.K4.htp=[ transport http ]
May  2 14:47:40.880: %PNPA-DHCP Op-43 Msg: _pdgfa.1.Ix.srv.ip.rm=[ 10.1.3.73 ]
May  2 14:47:40.880: %PNPA-DHCP Op-43 Msg: _pdgfa.1.Jx.srv.rt.rm=[ port 80 ]
May  2 14:47:40.880: %PNPA-DHCP Op-43 Msg: _pdoop.1.ztp=[pnp-zero-touch] host=[] ipad=[10.1.3.73]
port=80
May  2 14:47:40.880: %PNPA-DHCP Op-43 Msg: _pors.done=1
May  2 14:47:40.880: %PNPA-DHCP Op-43 Msg: _pdokp.1.kil=[PNPA_DHCP_OP43] pid=470 idn=[Vlan90]
May  2 14:47:40.880: XML-UPDOWN: Vlan90 XML Interface(102) SHUTDOWN(101). PID=470
May  2 14:47:41.674: DHCP: No configured hostname - not including Hostname option
May  2 14:47:41.677: %PNPA-DHCP Op-43 Msg: Op43 has 5A. It is for PnP
May  2 14:47:41.681: %PNPA-DHCP Op-43 Msg: After stripping extra characters in front of 5A, if any:
5A1D;B2;K4;I10.1.3.73;J80 op43_len: 25

May  2 14:47:41.681: %PNPA-DHCP Op-43 Msg: _pdoon.2.ina=[Vlan90]
May  2 14:47:41.681: %PNPA-DHCP Op-43 Msg: _papdo.2.cot=[5A1D;B2;K4;I10.1.3.73;J80]
lot=[5A1D;B2;K4;I10.1.3.73;J80]
May  2 14:47:41.681: %PNPA-DHCP Op-43 Msg: Process state = READY
May  2 14:47:41.681: %PNPA-DHCP Op-43 Msg: OK to process message
May  2 14:47:41.681: XML-UPDOWN: PNPA_DHCP_OP43 XML Interface(102) UP. PID=470
May  2 14:47:41.681: %PNPA-DHCP Op-43 Msg: _pdoon.2.ntf.don=470
May  2 14:47:41.681: %PNPA-DHCP Op-43 Msg: _pdoop.2.org=[A1D;B2;K4;I10.1.3.73;J80]
May  2 14:47:41.681: %PNPA-DHCP Op-43 Msg: _pdgfa.2.inp=[B2;K4;I10.1.3.73;J80]
May  2 14:47:41.681: %PNPA-DHCP Op-43 Msg: _pdgfa.2.B2.s12=[ ipv4 ]
May  2 14:47:41.681: %PNPA-DHCP Op-43 Msg: _pdgfa.2.K4.htp=[ transport http ]
May  2 14:47:41.681: %PNPA-DHCP Op-43 Msg: _pdgfa.2.Ix.srv.ip.rm=[ 10.1.3.73 ]
May  2 14:47:41.681: %PNPA-DHCP Op-43 Msg: _pdgfa.2.Jx.srv.rt.rm=[ port 80 ]
May  2 14:47:41.681: %PNPA-DHCP Op-43 Msg: _pdoop.2.ztp=[pnp-zero-touch] host=[] ipad=[10.1.3.73]
port=80
May  2 14:47:41.681: %PNPA-DHCP Op-43 Msg: _pors.done=1
May  2 14:47:41.684: %PNPA-DHCP Op-43 Msg: _pdokp.2.kil=[PNPA_DHCP_OP43] pid=470 idn=[Vlan90]
May  2 14:47:41.684: XML-UPDOWN: Vlan90 XML Interface(102) SHUTDOWN(101). PID=470
May  2 14:47:41.799: %DHCP-6-ADDRESS_ASSIGN: Interface Vlan90 assigned DHCP address 10.19.10.101,
mask 255.255.255.0, hostname

May  2 14:47:52.607: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/16, changed
state to down
May  2 14:47:53.607: %LINK-3-UPDOWN: Interface GigabitEthernet1/16, changed state to down
May  2 14:47:56.865: %PNP-6-HTTP_CONNECTING: PnP Discovery trying to connect to PnP server
http://10.1.3.73:80/pnp/HELLO
May  2 14:47:56.920: %PNP-6-HTTP_CONNECTED: PnP Discovery connected to PnP server
http://10.1.3.73:80/pnp/HELLO
May  2 14:47:57.123: %LINK-3-UPDOWN: Interface GigabitEthernet1/16, changed state to up
May  2 14:47:57.934: %PNP-6-PROFILE_CONFIG: PnP Discovery profile pnp-zero-touch configured
May  2 14:47:58.130: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/16, changed
state to up
May  2 14:48:14.356: %PNP-6-PNP_DISCOVERY_DONE: PnP Discovery done successfully
```

### Device Not Starting the Plug and Play Process

- Check that the device has no configuration. If the switch is a brownfield device, use the following commands to clear the switch configuration:

```
del flash:private-config.text

del flash:config.text

del sdflash:config.text

del pnp.dat

delete /f /r flash:dc_profile_dir

del *pnp*


configure terminal
no pnp profile pnp-zero-touch
do delete /force nvram:*.cer
do delete /force flash:pnp-reset-config.cfg
crypto key zeroize
yes
no crypto pki certificate pool
yes
no crypto pki trustpoint pnplabel
yes
end
write erase
```

- Check that the PnP VLAN was created automatically on the switch. Before the PnP process is started, you should see a log for an interface *VLAN pnp-VLAN* created on the IE switch:

```
May  2 14:47:36.672: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan90, changed state to up
```

If that is not the case, check that the EtherChannel is up on distribution switch and the PnP VLAN is configured and allowed on the trunk port.

- If the switch gets a DHCP IP, but the PnP process has not started, check that option 43 is configured on the DHCP server and that Option 60 is supported on the DHCP server.
- If a PnP timeout occurs while contacting Cisco DNA Center, check that Cisco DNA Center is reachable from the PnP VLAN.

### PnP Process Not Successful

Navigate to **Provision > Devices > Plug and Play** and click the device name. Under the **History** tab, check error details and click **Info** to get more information.

- If an error occurs while upgrading the device to the golden image, try to onboard but skip the golden image upgrade.
- If PnP process fails due to template configuration, try to paste the configuration template directly into the device CLI to identify template errors. If an error is found, adjust the template accordingly.

# Adding Brownfield Devices to the Cisco DNA Center

With Cisco DNA Center, you can add and provision brownfield devices to the network. Brownfield refers to devices that belong to existing sites with pre-existing infrastructure.

To add devices, run a **Discovery** job on the device. The **Discovery** feature scans the devices in your network and sends the list of discovered devices to **Inventory**. The Discovery feature can also work with the **Device Controllability** feature to configure the required network settings on devices if these settings are not already present on the device.

For more information about Device Controllability, see the *Cisco Digital Network Architecture Center Administrator Guide* at the following URL:

- https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-maintenance-guides-list.html

## Discovery Requirements

- Check the **Supported Devices List** for device support.
- Make sure network latency of the device is below the documented maximum, as stated in the *Cisco Digital Network Architecture Center Administrator Guide*.
- SNMP credentials should be configured on devices for use by the Cisco DNA Center.
- Configure SSH credentials on the devices you want the Cisco DNA Center to discover and manage. The Cisco DNA Center discovers and adds a device to its inventory if at least one of the following two criteria are met:
  - The account that is being used by Cisco DNA Center to SSH into your devices has privileged EXEC mode (level 15).
  - You configure the device's enable password as part of the CLI credentials configured in the Discovery job.
- The device must be reachable from the Cisco DNA Center.

## Creating a Discovery Job

Three ways exist for discovering a device: Cisco Discovery Protocol, IP address range, and link layer discovery protocol (LLDP). The following steps use the IP address range. For information on the other methods, see the *Cisco Digital Network Architecture Center Administrator Guide*.

1. Navigate to the **Cisco DNA Center dashboard**. Under the **Tools** section, click **Discovery** and supply a discovery name. Click **Range** and enter start and end IP addresses.

   If you have any additional ranges, next to the first range click **+**, enter the additional range, and repeat for any remaining ranges. Verify the credentials to be used for the discovery, and then at the bottom, click **Start**. The discovery details are displayed while the discovery runs.

2. If any discovery failures exist, inspect the devices list, resolve the problem, and restart the Discovery for those devices.

3. After the discovery process finishes successfully, navigate to the **Cisco DNA Center dashboard**. Under **Tools**, click **Inventory**. The discovered devices are displayed. After inventory collection completes, the devices show a status of **Managed**.

The Cisco DNA Center can now access the devices, synchronize the inventory, and make configuration changes on the devices.

**Tip:** On the right side of the title row for the Inventory table, you can temporarily adjust which columns are displayed. Adding the **Device Role** column allows you to see the device role assigned by discovery based on device type and to adjust the role to best reflect the actual deployment of a device, such as access, distribution, core, or border router. Adjusting the role now can improve the appearance of the initial topology maps, versus adjusting the roles in later procedures.

## Troubleshooting a Discovery Job

If discovery fails, check the following settings:

- Check for IP address reachability from Cisco DNA Center to the device.
- Check username and password configuration in **Settings.**
- Check whether telnet or SSH option is properly selected.
- Check using manual telnet or SSH to the device from Cisco DNA Center or any other client.
- Check the Simple Network Management Protocol (SNMP) community configuration matches on switch and Cisco DNA Center.
- **Discovery View** will provide additional information.

# Provisioning Device in Inventory

When a device is provisioned in the inventory, the Cisco DNA Center configures the devices with the Cisco Identity Services Engine (ISE) server information that you defined. In addition, the Cisco DNA Center configures the devices on the ISE server and propagates any subsequent updates to the devices to ISE server.

Additionally, if you want to apply a Day-N template to a device, it should be done through the **Provision Wizard**.

1. From the **Cisco DNA Center dashboard**, choose **Provision > Devices**. The **Device Inventory** window displays.
2. Click the **Device Inventory** tab.
3. Click the check box adjacent to the device you want to provision.

4. From the **Action** drop-down list, choose **Provision**.
5. The **Assign Site** window displays. Assign a site for the device.
6. Click **Next** to proceed to the configuration window. Click **Next** again (no actions required).
7. If any Day-N templates are available for the device, the templates associated with the site through the network profile appear in the advanced configuration. Use the **Find** feature to quickly search for the device by entering the device name or expand the templates folder and select the template in the left pane. In the right pane, select values for the attributes that are bound to source from the drop-down lists.

   To export the template variables into a CSV file while deploying the template, click **Export** in the right pane. You can use the CSV file to make necessary changes in the variable configuration and import it into Cisco DNA Center by clicking **Import** in the right pane.
8. Click **Next** and then click **Deploy**.

After you provision a network device, ISE will securely communicate with it using the Protected Access Credential (PAC) keys. Any future logins to the device will be authenticated using ISE, including automated logins by the Cisco DNA Center as part of its processes. If ISE is not reachable (no RADIUS response), the Cisco DNA Center uses the local login credentials.

**Warning:** Inventory provisioning for IE2000, IE3300, and IE3200 is not available in Cisco DNA Center 1.2.10. Trying to provision the device will result in an error; as a workaround, add needed configurations to the onboarding template or configure any required changes by CLI. This issue is addressed in Cisco DNA Center 1.3.

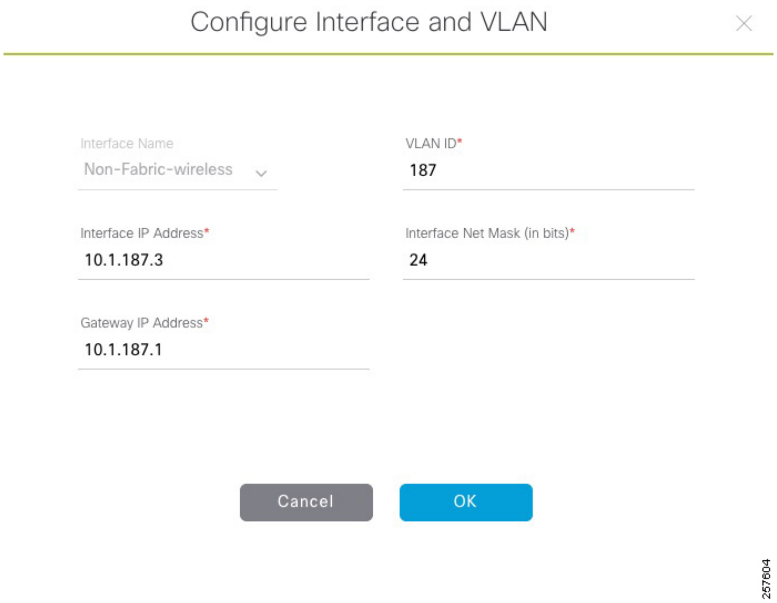
## Provisioning Wireless Access Points

This guide assumes that the administrator already discovered, configured redundancy, and upgraded the WLC. For more information on those tasks, refer to the *CVD Software-Defined Access Deployment Guide*.

The following process will push the configuration to the WLC:

1. Navigate to **PROVISION > Devices**.
2. Find the WLC and click the checkbox next to it, and then at the top of the screen under the **Actions** pull-down menu, select **Provision**. The **Provision Devices wizard** opens.
3. Assign the site and click **Next**. At the **Configuration** screen under **Managed AP Location**, select the additional floor assignments for APs managed by the WLC.
4. Select **+Add** in the interface section to create a WLC interface.
5. Complete the interface and VLAN configuration.

**Figure 12 WLC Interface Configuration**



Configure Interface and VLAN

Interface Name: Non-Fabric-wireless

VLAN ID*: 187

Interface IP Address*: 10.1.187.3

Interface Net Mask (in bits)*: 24

Gateway IP Address*: 10.1.187.1

6. Click **Next**, and then at the **Advanced Configuration** page, click **Next**.
7. At the **Summary** page, review the configurations. Click **Deploy**, and, at the slide-out panel, keep the default selection **Now**. Then click **Apply**. The WLC is assigned to the site and the provisioning starts. Click **Refresh** until the **Provision Status** shows **Success** before proceeding.

## AP Provision

In order to add APs to the network, you must do the following:

- Add DHCP scope for APs with option 43 pointing to WLC.
- Add IP helper address on distribution switch.
- Configure IE switch port as access with AP VLAN via CLI or Day-N template.
- Ensure the AP is connected to Power over Ethernet (PoE) port on IE switch or a power injector.

Follow this procedure to provision an AP:

1. Navigate to the **Cisco DNA Center dashboard**, and, under **Tools**, select **Inventory**. Select the WLC being added, and then at the top in the **Actions** drop-down list, select **Resync**. The APs associated with the WLC are added to the inventory without waiting for an inventory refresh.
2. Navigate to the **Cisco DNA Center dashboard**, and from **PROVISION > Devices > Inventory**, select the APs being added. At the top, in the **Actions** drop-down menu, select **Provision**.
3. On the **Provision Devices** page, assign the APs to a floor (the floor should be managed by a WLC), and then click **Next**. For RF Profile, select **TYPICAL** and then click **Next**.
4. At the **Summary** page, click **Deploy**. In the slide-out panel, leave the default selection of **Now**, and then click **Apply** and acknowledge any warnings about reboots.

# Provisioning a Software Image

The Cisco DNA Center allows you to push software images to the devices in your network. Prior to pushing the image, the Cisco DNA Center checks the device for upgrade readiness, including device management status, SCP and HTTPS file transfer success, and disk space. If any pre-checks fail, you cannot perform the software image update. After the software image of the device is upgraded, the Cisco DNA Center checks the CPU usage, route summary, and so on, to ensure that the state of the network remains unchanged after the image upgrade.

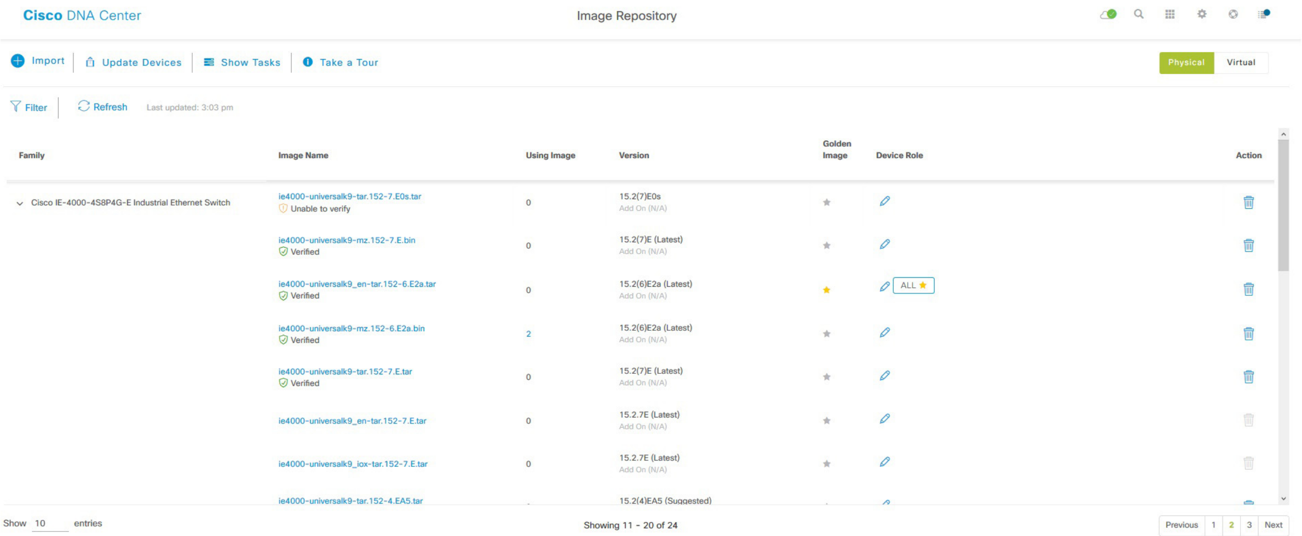
The Cisco DNA Center also compares each device's software image with the image that you have designated as golden for that specific device type. If a difference exists between the software image of the device and the golden image, then the Cisco DNA Center specifies the software image of the device as outdated. The upgrade readiness pre-checks will be triggered for those devices. If all the pre-checks are cleared, you can distribute the new image to the device and activate it. The activation of the new image requires a reboot of the device. This might interrupt the current network activity; if downtime is not feasible, you can schedule the process to a later time. If you have not designated a golden image for the device type, then the device's image cannot be updated.

## Designating an Image as Golden

To upgrade a device using the Cisco DNA Center, it must have a golden image for its platform. Devices can be assigned a golden image by **Family** and **Role**. When an image is marked as golden, it can be tagged so that it applies to a subset of devices by network role. The default is tag is **All**, but you can select from the following options: Core, Distribution, Border Router, Unknown, and Access.

1. Navigate to **Design > Image Repository**.
2. Navigate to the device family and then click the arrow next to the device family name to display a selection of images. Click the gray star under **Golden Image** to mark the image as golden.
   - If the software image is already imported to the Cisco DNA Center (indicated by a blue trashcan in the **Action** column), the process to mark it as golden is faster.
   - If the image is not imported (indicated by a gray trashcan), the process will take longer since DNA attempts to import the image directly from Cisco.com.

**Figure 13 Golden Image**



| Family | Image Name | Using Image | Version | Golden Image | Device Role | Action |
|---|---|---|---|---|---|---|
| Cisco IE-4000-4S8P4G-E Industrial Ethernet Switch | ie4000-universalk9-tar.152-7.E0s.tar<br>Unable to verify | 0 | 15.2(7)E0s<br>Add On (N/A) | ☆ | ✎ | 🗑 |
| | ie4000-universalk9-mz.152-7.E.bin<br>Verified | 0 | 15.2(7)E (Latest)<br>Add On (N/A) | ☆ | ✎ | 🗑 |
| | ie4000-universalk9_en-tar.152-6.E2a.tar<br>Verified | 0 | 15.2(6)E2a (Latest)<br>Add On (N/A) | ★ | ✎ ALL ★ | 🗑 |
| | ie4000-universalk9-mz.152-6.E2a.bin<br>Verified | 2 | 15.2(6)E2a (Latest)<br>Add On (N/A) | ☆ | ✎ | 🗑 |
| | ie4000-universalk9-tar.152-7.E.tar<br>Verified | 0 | 15.2(7)E (Latest)<br>Add On (N/A) | ☆ | ✎ | 🗑 |
| | ie4000-universalk9_en-tar.152-7.E.tar | 0 | 15.2.7E (Latest)<br>Add On (N/A) | ☆ | ✎ | 🗑 |
| | ie4000-universalk9_iox-tar.152-7.E.tar | 0 | 15.2.7E (Latest)<br>Add On (N/A) | ☆ | ✎ | 🗑 |
| | ie4000-universalk9-tar.152-4.EA5.tar | - | 15.2(4)EA5 (Suggested) | | | |

## Upgrading Device to Golden Image

1. To check if a device needs upgrading, navigate to **Provision > Devices > Inventory**.

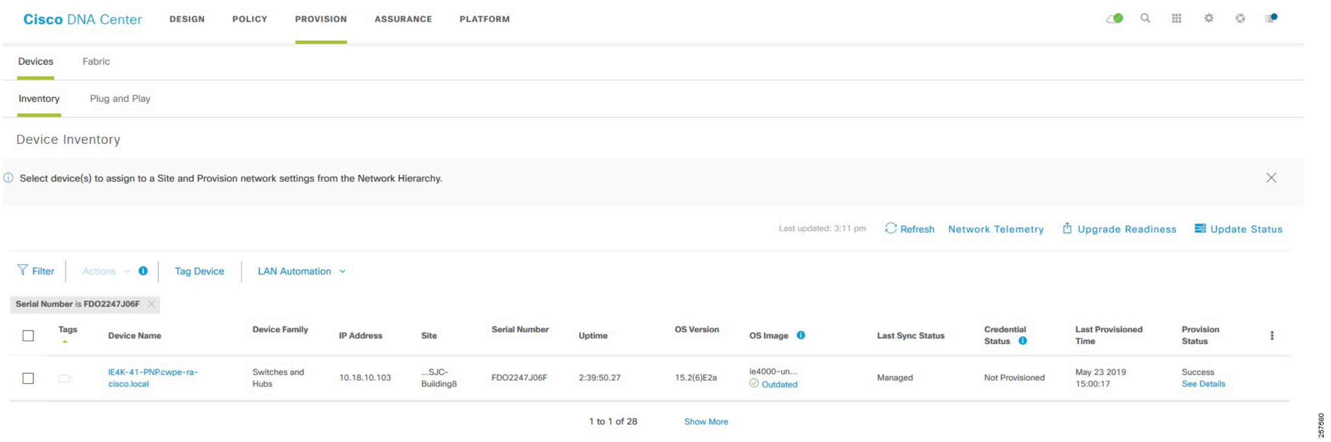
   – If a device shows as **Outdated** in the OS Image field, the device is not on the golden image and should be updated.

   – If there is a **green check mark** next to **Outdated**, the device has passed upgrade readiness checks and can be updated.

   – If there is a **red X mark** next to **Outdated**, the device has one or more issues in its readiness checks that must be resolved before the device can be updated.

   – If **Outdated** is not displayed in the OS Image field for a device, it is either on the golden image or does not have a golden image specified in **Design > Image Repository**.

**Figure 14 Upgrade Readiness**



Select device(s) to assign to a Site and Provision network settings from the Network Hierarchy.

Serial Number is FDO2247J06F

| ☐ | Tags | Device Name | Device Family | IP Address | Site | Serial Number | Uptime | OS Version | OS Image | Last Sync Status | Credential Status | Last Provisioned Time | Provision Status |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | | IE4K-41-PNP.cwpe-ra-cisco.local | Switches and Hubs | 10.18.10.103 | ...SJC-Building8 | FDO2247J06F | 2:39:50.27 | 15.2(6)E2a | ie4000-un...<br>✓ Outdated | Managed | Not Provisioned | May 23 2019 15:00:17 | Success<br>See Details |

1 to 1 of 28 Show More

2. (Only if necessary) For more detail on a device's image upgrade readiness check, click **Outdated**. The **Image Upgrade Readiness Check** window appears. Near the top of the page, the current running image and the golden image are displayed. The **Check Type** field lists the readiness check, and a brief description is shown. One or more failures will prevent provisioning of an image and need to be corrected before the image can be updated. Warning triangles in the **Status** field indicate an issue, but do not affect the ability to provision a software image to the device. Once issues are corrected, proceed to the next step.

   **Tip:** If you correct an issue on a device, click **Recheck**, and if the issue still displays a failing status, resync the device on the inventory page using **Actions > Resync** to update device details in the Cisco DNA Center. The change may be made on the device, but might not have populated to the Cisco DNA Center.

**Figure 15 Image Upgrade Readiness Check**

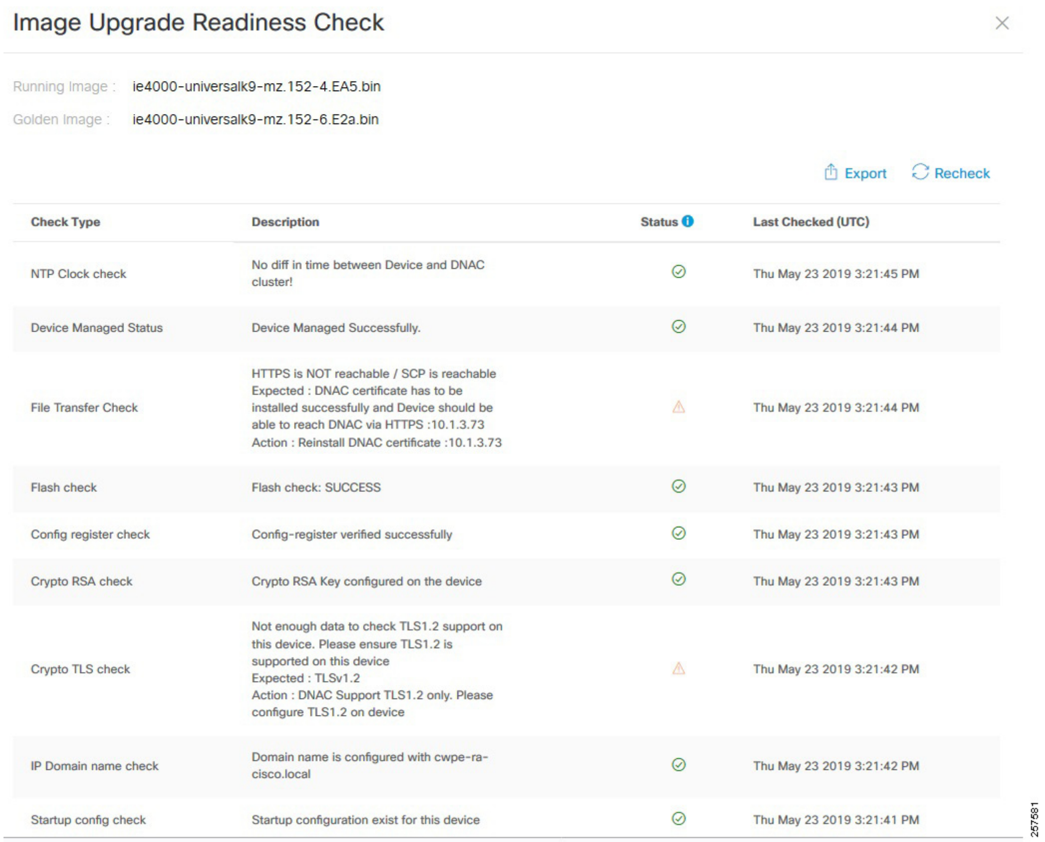


Image Upgrade Readiness Check

Running Image : ie4000-universalk9-mz.152-4.EA5.bin

Golden Image : ie4000-universalk9-mz.152-6.E2a.bin

| Check Type | Description | Status | Last Checked (UTC) |
|---|---|---|---|
| NTP Clock check | No diff in time between Device and DNAC cluster! | ✓ | Thu May 23 2019 3:21:45 PM |
| Device Managed Status | Device Managed Successfully. | ✓ | Thu May 23 2019 3:21:44 PM |
| File Transfer Check | HTTPS is NOT reachable / SCP is reachable<br>Expected : DNAC certificate has to be installed successfully and Device should be able to reach DNAC via HTTPS :10.1.3.73<br>Action : Reinstall DNAC certificate :10.1.3.73 | ⚠ | Thu May 23 2019 3:21:44 PM |
| Flash check | Flash check: SUCCESS | ✓ | Thu May 23 2019 3:21:43 PM |
| Config register check | Config-register verified successfully | ✓ | Thu May 23 2019 3:21:43 PM |
| Crypto RSA check | Crypto RSA Key configured on the device | ✓ | Thu May 23 2019 3:21:43 PM |
| Crypto TLS check | Not enough data to check TLS1.2 support on this device. Please ensure TLS1.2 is supported on this device<br>Expected : TLSv1.2<br>Action : DNAC Support TLS1.2 only. Please configure TLS1.2 on device | ⚠ | Thu May 23 2019 3:21:42 PM |
| IP Domain name check | Domain name is configured with cwpe-ra-cisco.local | ✓ | Thu May 23 2019 3:21:42 PM |
| Startup config check | Startup configuration exist for this device | ✓ | Thu May 23 2019 3:21:41 PM |

3. To begin the image update process, click the check box next to one or more devices that require an image update and that have passed image update pre-checks. Then click **Actions > Update OS Image**. The **OS Update** window will display.

4. At the **Distribute** step, select the radio button next to **Now** to begin distribution of the image immediately or **Later** to schedule distribution for later. Click **Next** to continue to the **Activate** step. During device sync, the Cisco DNA Center checks files in the target device file system. If the golden image is found in the file system, the distribution step will be skipped.

5. At the **Activate** step, click the check box next to **Schedule Activation after Distribution is completed** to reload the device and boot to the new image immediately after distribution is complete. Leave the box unchecked to pre-stage the image on the device and schedule image activation and device reload for a later time. Click **Next** to continue to the **Confirm** step.

6. At the **Confirm** step, review details entered for image upgrade. Click **Confirm** to submit.

When an image upgrade begins, click **Upgrade Status** in the upper right corner of **Provision > Inventory > Devices** to bring up the **Recent Tasks** page in order to view the status of ongoing and previously completed upgrades. Click the drop-down arrow to the far right of each entry in **Recent Tasks** to display more information about distribution and activation operations.

Click **Refresh** periodically to see the most up-to-date information on job status. When complete, both the distribution operation and activate operation are preceded by green check marks and the top-level status is successful.

**Figure 16 Successful Software Upgrade**

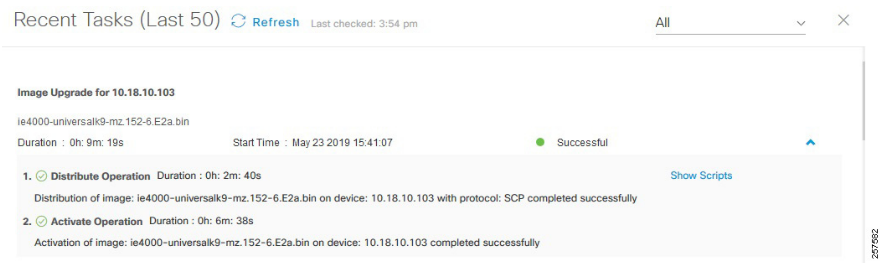


**Image Upgrade for 10.18.10.103**

ie4000-universalk9-mz.152-6.E2a.bin

Duration : 0h: 9m: 19s Start Time : May 23 2019 15:41:07 ● Successful

1. ✓ **Distribute Operation** Duration : 0h: 2m: 40s

   Distribution of image: ie4000-universalk9-mz.152-6.E2a.bin on device: 10.18.10.103 with protocol: SCP completed successfully

2. ✓ **Activate Operation** Duration : 0h: 6m: 38s

   Activation of image: ie4000-universalk9-mz.152-6.E2a.bin on device: 10.18.10.103 completed successfully

Once upgraded to the golden image, outdated no longer appears in the OS Image field for the device in inventory.

**Tips:**

- If distribution of an image fails, ensure that SSH version 2 is enabled on the device.
- If activation fails for any reason, you can retry by creating a new task. The Cisco DNA Center will find the image in the device already and distribution step will be skipped.

**Warning:** Images with language support in which the name in the .tar file differs from the name in the .bin file is not supported in Cisco DNA Center 1.2.10. As an alternative, use an image without language support. This limitation is removed in Cisco DNA Center 1.3.

# Security

This section will guide you through configurations needed on the Cisco DNA Center, IE switches, WLC, and ISE to provide the security measures presented in the *Extended Enterprise Design Guide*, including:

- Creating intent-based security policies in the Cisco DNA Center
- Configuring Cisco TrustSec on the network components
- Enabling endpoint visibility on the network

## Intent-Based Security Policy

Intent-based security gives the administrator the ability to express operational intent and automatically have the system select the appropriate IT-defined security policies without requiring network or security skills.

As part of the design decisions in advance of your network deployment, you decide network segmentation strategies for the organization. Micro-segmentation uses scalable group tags to apply policy to groups of users or device profiles. The desired outcomes of policy application using segmentation may be easily accommodated with group policies. In an Extended Enterprise example, 802.1x-authenticated users may be permitted to access network resources, but Internet of Things (IoT) devices may be limited to only specific server or services to avoid any network intrusion.

### Create a Micro-segmentation Policy using Scalable Group Tags

Micro-segmentation creates network segmentation that relies on the use of role- or group-based membership, regardless of IP addressing, in order to create policies that allow segmentation in the network.

Micro-segmentation policies are customized for an organization's deployment. The following example shows a basic policy that can be used to deny IP cameras communication with other IP cameras.

1. From the **Cisco DNA Center** dashboard, navigate to **POLICY > Group-Based Access Control > Group-Based Access Control Policies**.

2. Click **+ Add Policy**.

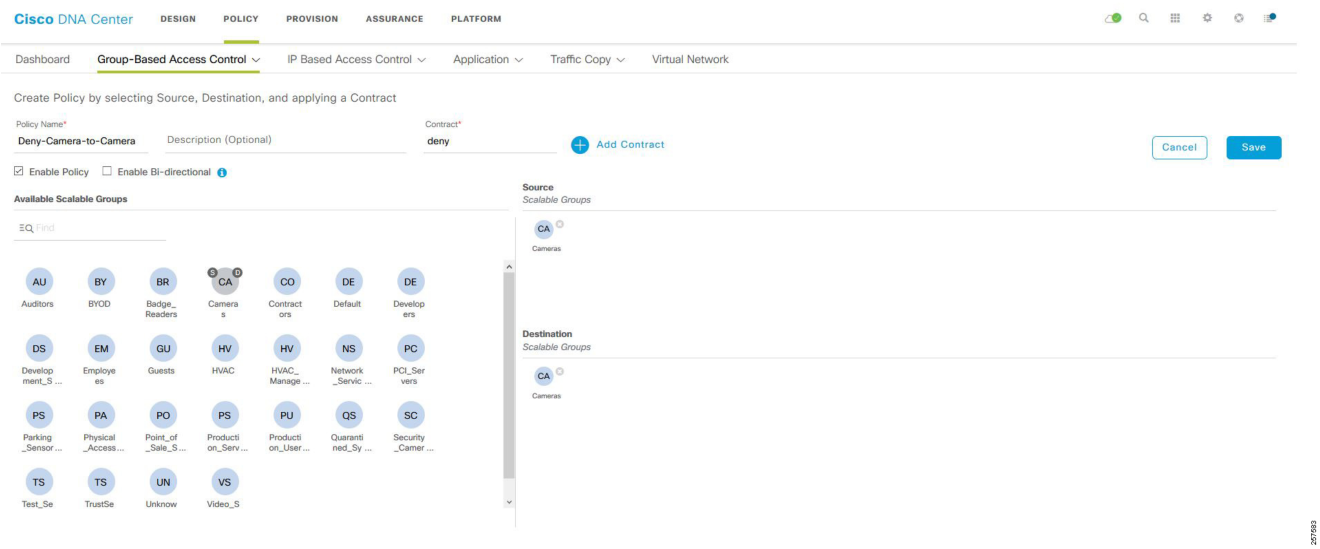
3. From the **Available Scalable Groups** pane, drag the **Cameras** group and drop it into the **Source** pane. Next, drag the **Cameras** group into the **Destination** pane. Enter a policy name (example: Deny-Camera-to-Camera) and a description, and then click the **Enable Policy** check box.

4. Click **+ Add Contract** and select **Deny**. Click **OK** and then click **Save**.

   **Tip:** Enabling Bi-directional will create two policies; the second one will have the opposite source and destination.

   The policy is created and listed with a status of **DEPLOYED**. The policies are now available in ISE in the TrustSec policy matrix.

**Figure 17 Creating Security Policy**



Create Policy by selecting Source, Destination, and applying a Contract

Policy Name*: Deny-Camera-to-Camera

Description (Optional)

Contract*: deny

☑ Enable Policy ☐ Enable Bi-directional

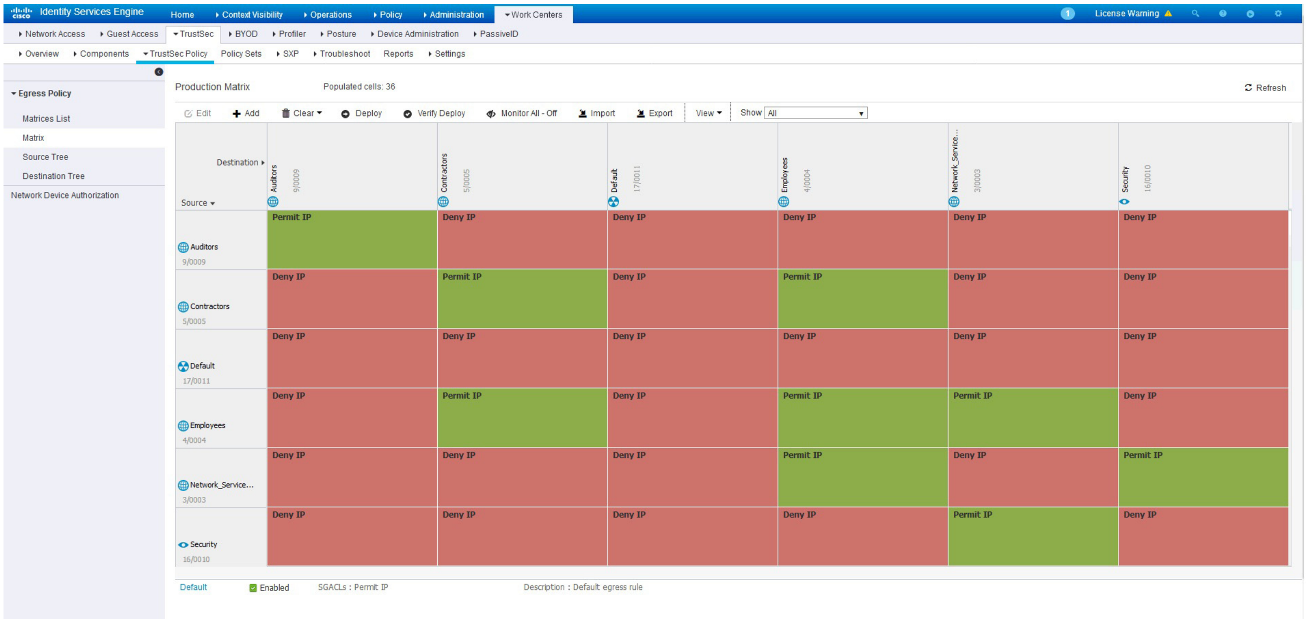
Source Scalable Groups: CA Cameras

Destination Scalable Groups: CA Cameras

5. At the top right of the **Group-based Access Control Policies** page, click **Advanced Options**. You are redirected to log in to ISE, which then displays the TrustSec policy matrix. Verify that the policy has been updated to ISE for distribution to the network devices.

   This step is a shortcut to logging in to ISE, navigating to **Work Centers > TrustSec > TrustSec Policy**.

## Figure 18 TrustSec Policy Matrix



Production Matrix Populated cells: 36

Show All

| Source ▾ \ Destination ▸ | Auditors 9/0009 | Contractors 5/0005 | Default 17/0011 | Employees 4/0004 | Network_Service... 3/0003 | Security 16/0010 |
|---|---|---|---|---|---|---|
| Auditors 9/0009 | Permit IP | Deny IP | Deny IP | Deny IP | Deny IP | Deny IP |
| Contractors 5/0005 | Deny IP | Permit IP | Deny IP | Permit IP | Deny IP | Deny IP |
| Default 17/0011 | Deny IP | Deny IP | Deny IP | Deny IP | Deny IP | Deny IP |
| Employees 4/0004 | Deny IP | Permit IP | Deny IP | Permit IP | Permit IP | Deny IP |
| Network_Service... 3/0003 | Deny IP | Deny IP | Deny IP | Permit IP | Deny IP | Permit IP |
| Security 16/0010 | Deny IP | Deny IP | Deny IP | Deny IP | Permit IP | Deny IP |

Default ☑ Enabled SGACLs : Permit IP Description : Default egress rule

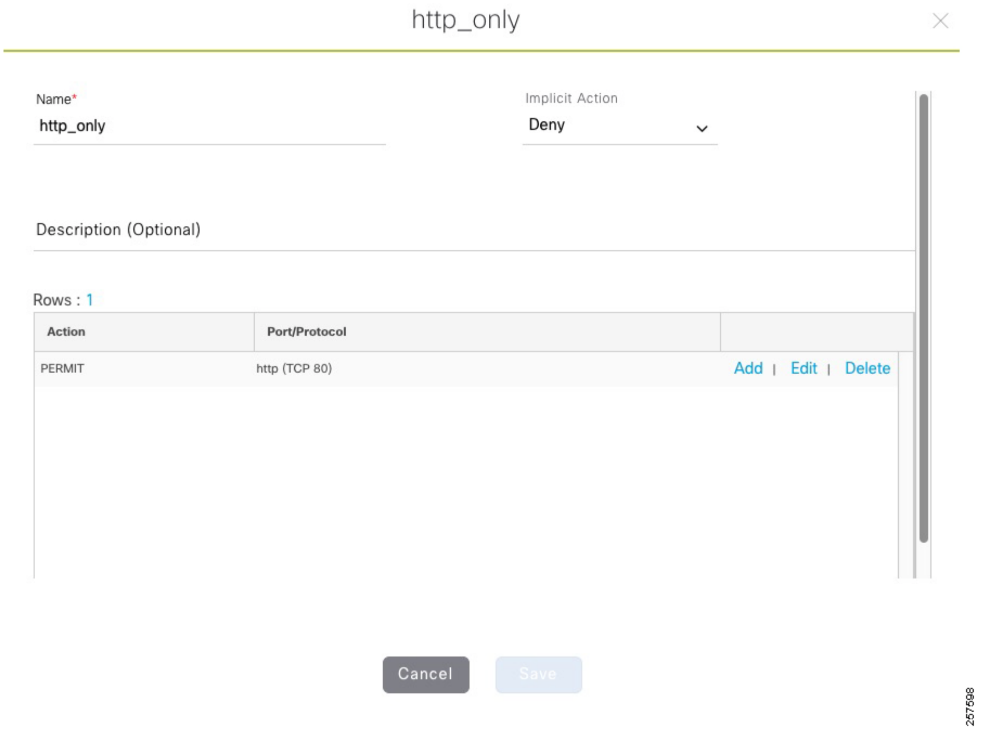
257740

## Creating Custom Contracts

The two default options for policy enforcement are **permit** and **deny**; however, it is possible to create custom contracts for more granularity. After creating a contract, it can be used in security policies.

1. Navigate to **Group-Based Access Control > Access Contract**.
2. Click **Add contract**.

**Figure 19 Custom Contracts**



http_only

Name*: http_only

Implicit Action: Deny

Description (Optional)

Rows : 1

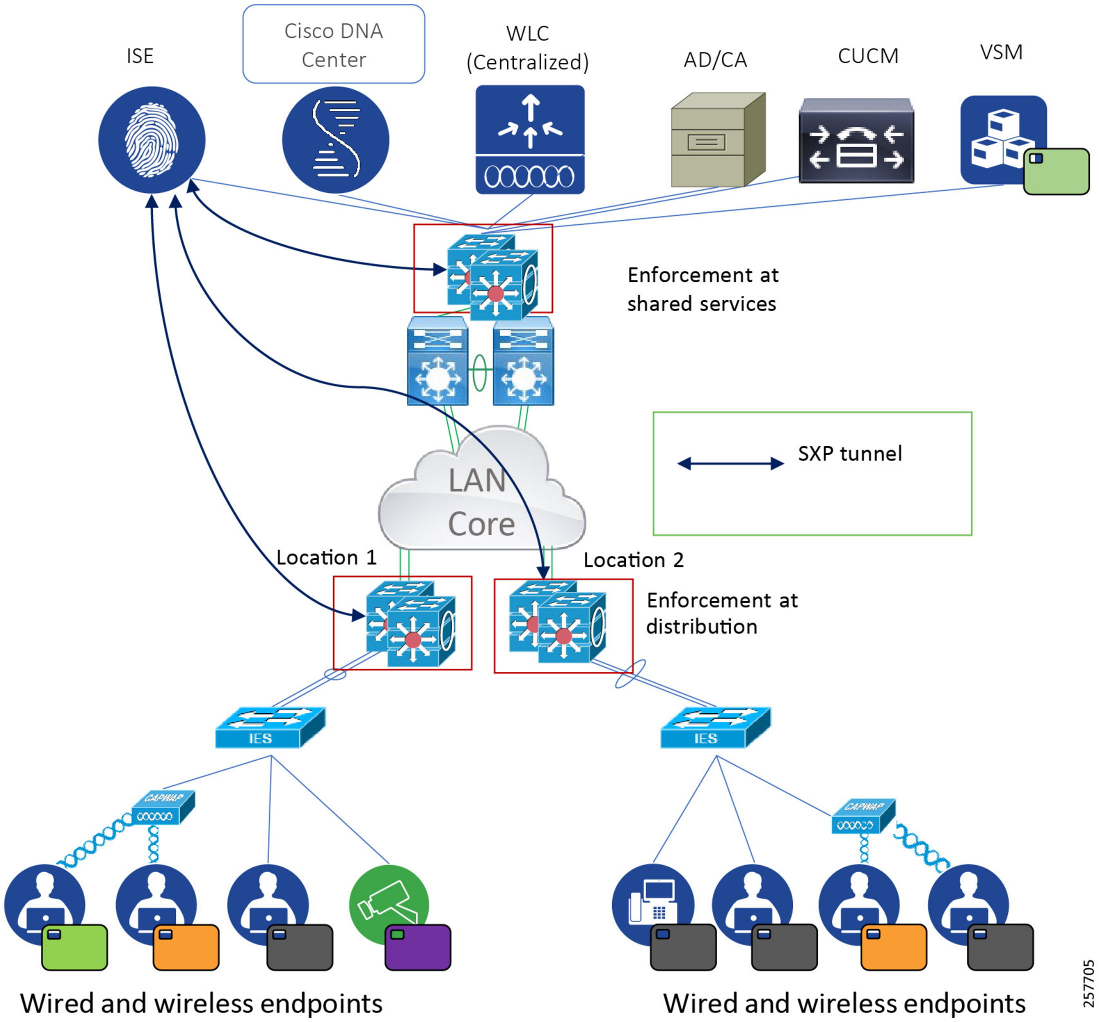
| Action | Port/Protocol | |
|---|---|---|
| PERMIT | http (TCP 80) | Add \| Edit \| Delete |

## Configuring TrustSec on Network Components

TrustSec assigns Scalable Group Tags (SGTs) to wired or wireless endpoints when they connect to a network. By using these tags, an IT security architect can define and enforce an access policy on any networking device. TrustSec is defined in three phases: classification, propagation, and enforcement. When the endpoint joins the network, its SGT gets propagated in the network to the enforcement points that control traffic based on tag information and policies.

Figure 20 illustrates the TrustSec implementation used in this CVD. Classification is done using authentication and authorization policies in ISE, and propagation of tags on the network is achieved using SGT Exchange Protocol (SXP) tunnels between ISE and devices used as enforcement points. Enforcement points in this design are distribution switches and the shared services switch. For more information on security design, refer to the *Extended Enterprise Design Guide*.

**Figure 20 TrustSec Implementation**


ISE
Cisco DNA Center
WLC (Centralized)
AD/CA
CUCM
VSM
Enforcement at shared services
SXP tunnel
LAN Core
Location 1
Location 2
Enforcement at distribution
IES
IES
CAPWAP
CAPWAP
Wired and wireless endpoints
Wired and wireless endpoints
257705

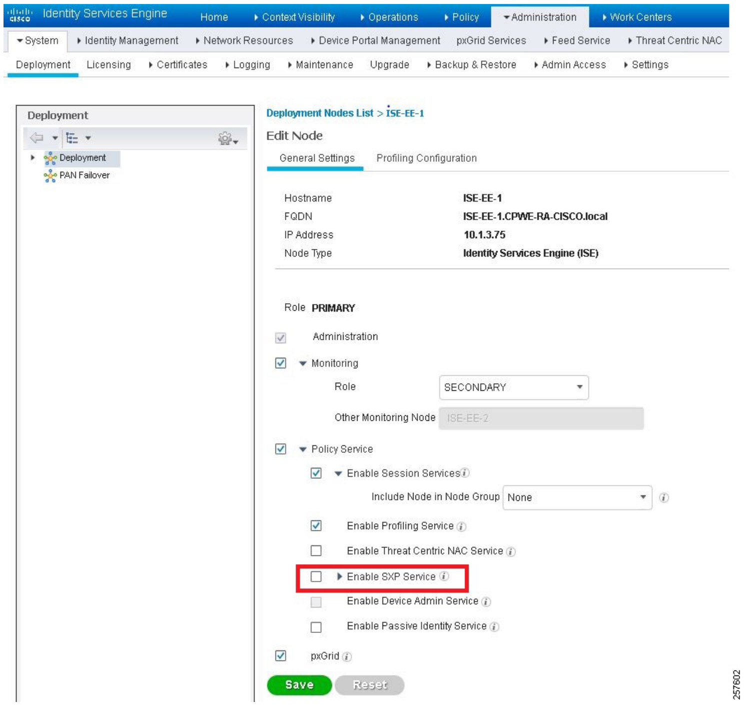
## Configuring TrustSec in Cisco ISE

For Cisco ISE to assign SGTs to endpoints, IE switch details such as IP address and RADIUS pre-shared secret key must be configured on Cisco ISE. The TrustSec configuration should also be applied to the Cisco switch. This step is done automatically when provisioning the device in inventory as described in Provisioning Device in Inventory, page 21.

## Configuring SXP in Cisco ISE

Enable the SXP service in Cisco ISE by navigating to **Administration > Deployment**. Click the **Enable SXP Service** check box if it is unchecked, and then click **Save**.

### Figure 21 Enabling SXP Service



Hostname ISE-EE-1

FQDN ISE-EE-1.CPWE-RA-CISCO.local

IP Address 10.1.3.75

Node Type Identity Services Engine (ISE)

Role PRIMARY

☑ Administration

☑ Monitoring

Role SECONDARY

Other Monitoring Node ISE-EE-2

☑ Policy Service

☑ Enable Session Services

Include Node in Node Group None

☑ Enable Profiling Service

☐ Enable Threat Centric NAC Service

☐ Enable SXP Service

☐ Enable Device Admin Service

☐ Enable Passive Identity Service

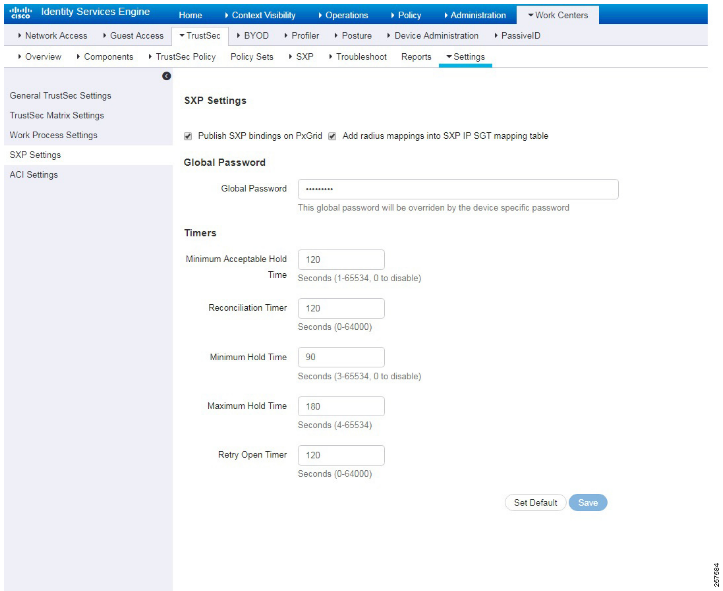
☑ pxGrid

## Configuring SXP Peers

The switches used for enforcement are configured as listeners and Cisco ISE is enabled as a speaker. To configure SXP peers, the source and the destination IP addresses must match at the switch and ISE. In ISE, a default configuration template can be used to fill in the rest of the parameters, such as password.

1. (Optional) In ISE, configure SXP default parameters at **Work Centers > TrustSec > Settings**. Select **SXP Settings** on the left panel and add a global password. Then click **Save**.

**Figure 22 SXP Settings**



SXP Settings

☑ Publish SXP bindings on PxGrid ☑ Add radius mappings into SXP IP SGT mapping table

Global Password

Global Password: ••••••••
This global password will be overriden by the device specific password

Timers

Minimum Acceptable Hold Time: 120
Seconds (1-65534, 0 to disable)

Reconciliation Timer: 120
Seconds (0-64000)

Minimum Hold Time: 90
Seconds (3-65534, 0 to disable)

Maximum Hold Time: 180
Seconds (4-65534)

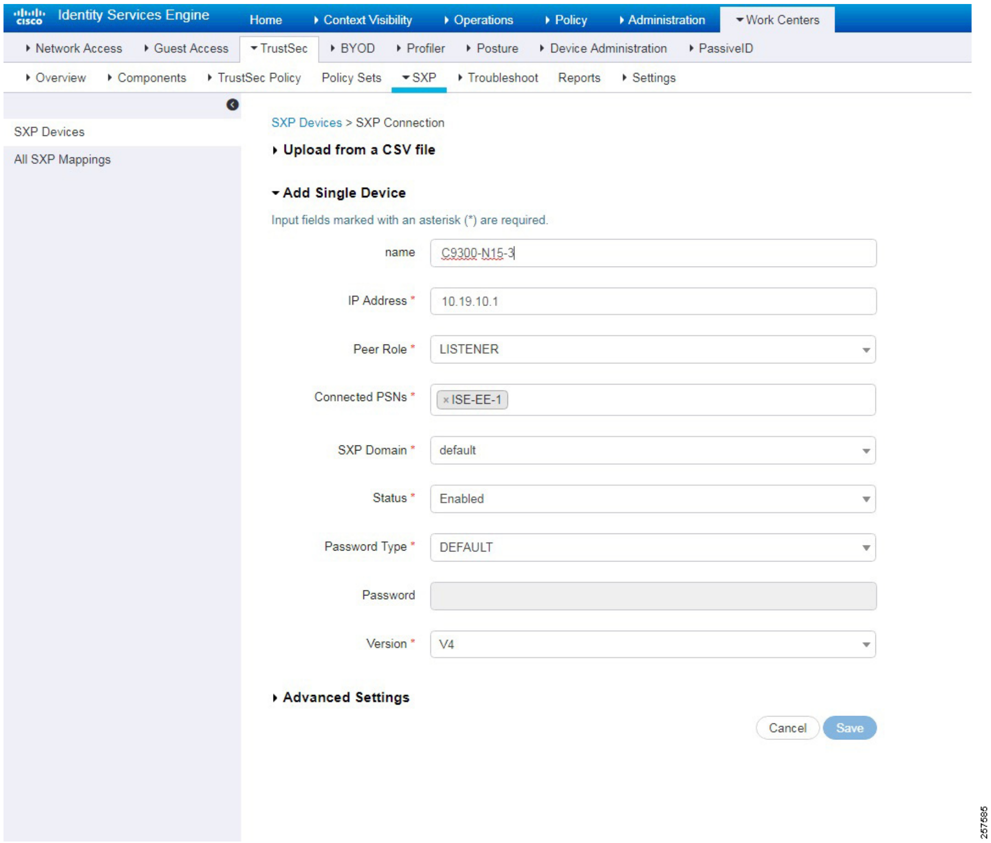
Retry Open Timer: 120
Seconds (0-64000)

2. Navigate to **Work Centers > TrustSec > SXP**.

3. Click **+Add**.

4. Add a name and IP address. In the **Peer Role** drop-down list, select **Listener**. In the **Connected PSNs** field, enter one or multiple appropriate Policy Service Nodes (PSNs) and then click **Save**.

**Figure 23 Adding SXP Device**



SXP Devices > SXP Connection

▸ Upload from a CSV file

▾ Add Single Device

Input fields marked with an asterisk (*) are required.

name: C9300-N15-3

IP Address *: 10.19.10.1

Peer Role *: LISTENER

Connected PSNs *: × ISE-EE-1

SXP Domain *: default

Status *: Enabled

Password Type *: DEFAULT

Password:

Version *: V4

▸ Advanced Settings

Matching SXP tunnel configuration on Cisco switches used for enforcement is covered in Configuring SXP in Cisco ISE, page 32.

## Configuring SGT Components on ISE

When ISE profiles, authenticates, and authorizes an endpoint device, ISE assigns an SGT to it. Endpoints connected to the network need to be grouped based on the device function, such as IP cameras and IP phones. In this CVD, a few device profiles were tested to illustrate SGT design examples. For details on user and device profiles, SGTs, and policies used in the Extended Enterprise design, refer to the *Extended Enterprise Design Guide*.

### Creating Scalable Group Tags

1. To create additional Security Groups in ISE, navigate to **Work Centers > TrustSec > Components** and select **Security Groups** on the left panel.

2. Click **+Add**.

3. Enter a name, select an icon, and add a description. Click **Submit**.

Cisco DNA Center communicates to ISE through REST API calls, and, as a result, the newly created security tags are available to use in Cisco DNA Center when configuring policies.

## Authentication Policy

Authentication policies define the protocols that Cisco ISE uses to communicate with the network devices, and the identity sources that it uses for authentication. A policy is a set of conditions and a result. ISE evaluates the policy conditions and, based on whether the result is true or false, applies the configured result. The authentication method tested in this CVD for IoT endpoints is called MAC Authentication Bypass (MAB). MAB uses the MAC address of a device to determine what kind of network access to provide. This method is used to authenticate end devices that do not support any supplicant software in them, such as 802.1X EAP-TLS, EAP-FAST, and so on.

For more information about MAB, refer to the following URL:

- https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-services/config_guide_c17-663759.html

The authentication policy used in Cisco ISE for this CVD checks the protocol and checks the internal identity store for the endpoint MAC address. To configure the authentication policy in ISE, navigate to **Policy > Policy Sets > Default** and select the arrow on the right to configure the authentication policy.

**Note:** In this CVD, the default authentication policy set is used.

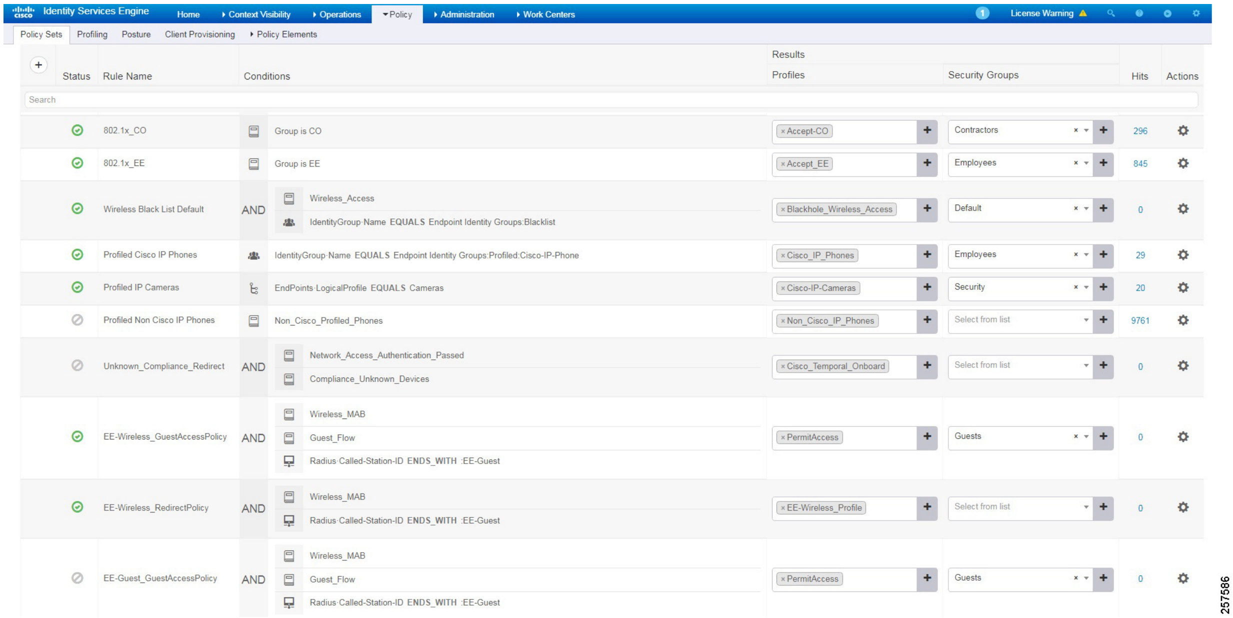
## Authorization Policies

Authorization policies are critical for determining what the user should access within the network. Authorization policies are composed of authorization rules and can contain conditional requirements that combine one or more identity groups. The permissions granted to the user are defined in authorization profiles, which act as containers for specific permissions.

Authorization profiles group the specific permissions granted to a user or a device and can include attributes such as an associated VLAN, access control list (ACL), or SGT. This CVD uses SGT to grant permissions to an IoT asset. The TrustSec Policy Matrix determines the permissions associated with each device.

To configure the authorization policy in ISE, navigate to **Policy > Policy Sets > Default** and then select **Authorization Policy**.

**Figure 24 Authorization Policies**



| Status | Rule Name | Conditions | Results |  | Hits | Actions |
|---|---|---|---|---|---|---|
|  |  |  | Profiles | Security Groups |  |  |
| ✓ | 802.1x_CO | Group is CO | Accept-CO | Contractors | 296 | ⚙ |
| ✓ | 802.1x_EE | Group is EE | Accept_EE | Employees | 845 | ⚙ |
| ✓ | Wireless Black List Default | AND<br>Wireless_Access<br>IdentityGroup·Name EQUALS Endpoint Identity Groups:Blacklist | Blackhole_Wireless_Access | Default | 0 | ⚙ |
| ✓ | Profiled Cisco IP Phones | IdentityGroup·Name EQUALS Endpoint Identity Groups:Profiled:Cisco-IP-Phone | Cisco_IP_Phones | Employees | 29 | ⚙ |
| ✓ | Profiled IP Cameras | EndPoints·LogicalProfile EQUALS Cameras | Cisco-IP-Cameras | Security | 20 | ⚙ |
| ⊘ | Profiled Non Cisco IP Phones | Non_Cisco_Profiled_Phones | Non_Cisco_IP_Phones | Select from list | 9761 | ⚙ |
| ⊘ | Unknown_Compliance_Redirect | AND<br>Network_Access_Authentication_Passed<br>Compliance_Unknown_Devices | Cisco_Temporal_Onboard | Select from list | 0 | ⚙ |
| ✓ | EE-Wireless_GuestAccessPolicy | AND<br>Wireless_MAB<br>Guest_Flow<br>Radius·Called-Station-ID ENDS_WITH :EE-Guest | PermitAccess | Guests | 0 | ⚙ |
| ✓ | EE-Wireless_RedirectPolicy | AND<br>Wireless_MAB<br>Radius·Called-Station-ID ENDS_WITH :EE-Guest | EE-Wireless_Profile | Select from list | 0 | ⚙ |
| ⊘ | EE-Guest_GuestAccessPolicy | AND<br>Wireless_MAB<br>Guest_Flow<br>Radius·Called-Station-ID ENDS_WITH :EE-Guest | PermitAccess | Guests | 0 | ⚙ |

The default policy can be designed based on the organization's specific security requirements. One option is to assign a default SGT like DEFAULT_GENERIC and classify devices that do not meet any of the authorization policy conditions. Or, in a more stringent design, if an endpoint asset is not being profiled by any of the existing conditions, then network access is denied.

# Configuring SGT Components on Industrial Switches

## Configure Authentication, Authorization, and Accounting

Industrial switches need an authentication, authorization, and accounting (AAA) configuration to allow the onboarding of endpoints. This step is done automatically when provisioning the device in inventory as described in Provisioning Device in Inventory, page 21.

## Configuring Port-based Authentication

This CVD uses identity control policies for port-based authentication, specifically **PMAP_DefaultWIredDot1xClosedAuth_MAB_1X**. Sample AAA policies shows a template for policy configuration that was used to the IE devices using Day-N templates.

The following example shows configuration of switchport access details on the port as well as authentication parameters.

```
interface GigabitEthernet1/13
 switchport voice vlan 93
 switchport access vlan 94
 switchport mode access
 authentication periodic
 authentication timer reauthenticate server
 access-session closed
 access-session port-control auto
 mab
 dot1x pae authenticator
 service-policy type control subscriber PMAP_DefaultWiredDot1xClosedAuth_MAB_1X
```

## Configuring Enforcement Points

As previously mentioned, enforcement is performed by the distribution and shared services switches. This section describes the steps to configure enforcement on the distribution switch.

### Configuring Cisco TrustSec Credentials and AAA

When provisioning the device in Cisco DNA Center inventory, the Cisco TrustSec device ID and the password for the switch to use when authenticating with Cisco ISE and establishing the PAC file and AAA settings are configured automatically. To provision the device, run a Discovery job as described in Creating a Discovery Job, page 21.

### Configuring SXP Tunnel

The SXP tunnel is required for SGT propagation from ISE to the enforcement point. The following is the SXP tunnel configuration on the IE switch:

```
Switch(config)#cts sxp enable
Switch(config)# cts sxp default password password_type_and_value
Switch(config)# cts sxp connection peer ISE_IP source LOCAL_IP password default mode local listener
hold-time 0 0
```

## Enabling Enforcement

To enable policy enforcement, the following commands must be enabled:

```
Switch(config)# cts role-based enforcement
Switch(config)# cts role-based enforcement vlan-list vlan
```

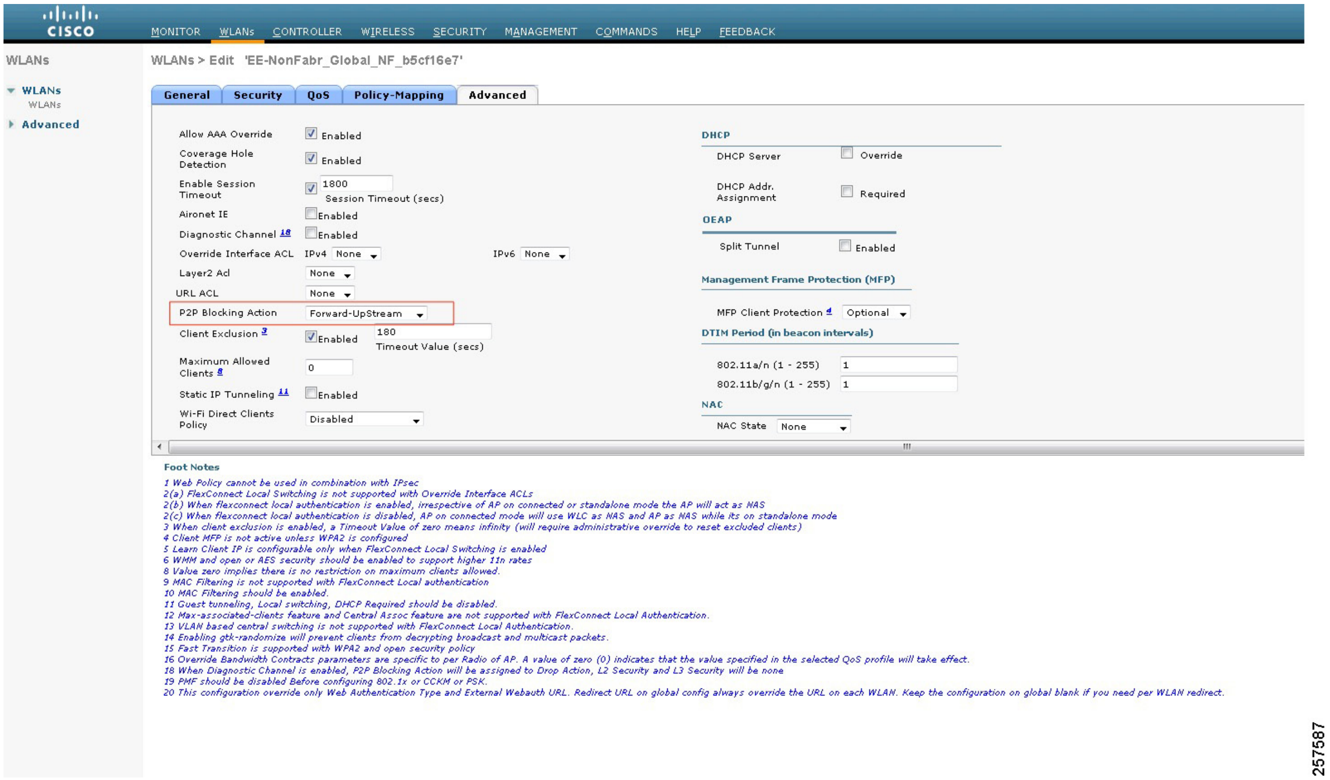
## Enforcement Considerations for Wireless Traffic

When using the configurations above, the wireless-to-wireless traffic is not subject to enforcement since it is tunneled. If enforcement is needed, the WLC needs to forward peer-to-peer traffic upstream to the attached switch for the enforcement to happen there. In this CVD, the WLC is connected to the shared services switch. The following describes the required configurations.

### Configure WLC to Forward Peer-to-Peer Traffic

1. On the **WLC administrator** page, navigate to **Advanced** at the upper right corner.
2. Navigate to **WLANs** and select the relevant SSID.
3. Click the **Advanced** tab.
4. For the **P2P Blocking Action**, select **Forward-UpStream**.

Figure 25 WLC P2P Forward-Upstream Configuration



WLANs > Edit 'EE-NonFabr_Global_NF_b5cf16e7'

Allow AAA Override ☑ Enabled

Coverage Hole Detection ☑ Enabled

Enable Session Timeout ☑ 1800 Session Timeout (secs)

Aironet IE □ Enabled

Diagnostic Channel 18 □ Enabled

Override Interface ACL IPv4 None IPv6 None

Layer2 Acl None

URL ACL None

P2P Blocking Action Forward-UpStream

Client Exclusion 3 ☑ Enabled 180 Timeout Value (secs)

Maximum Allowed Clients 8 0

Static IP Tunneling 11 □ Enabled

Wi-Fi Direct Clients Policy Disabled

DHCP

DHCP Server □ Override

DHCP Addr. Assignment □ Required

OEAP

Split Tunnel □ Enabled

Management Frame Protection (MFP)

MFP Client Protection 4 Optional

DTIM Period (in beacon intervals)

802.11a/n (1 - 255) 1

802.11b/g/n (1 - 255) 1

NAC

NAC State None

Foot Notes

1 Web Policy cannot be used in combination with IPsec
2(a) FlexConnect Local Switching is not supported with Override Interface ACLs
2(b) When flexconnect local authentication is enabled, irrespective of AP on connected or standalone mode the AP will act as NAS
2(c) When flexconnect local authentication is disabled, AP on connected mode will use WLC as NAS and AP as NAS while its on standalone mode
3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
4 Client MFP is not active unless WPA2 is configured
5 Learn Client IP is configurable only when FlexConnect Local Switching is enabled
6 WMM and open or AES security should be enabled to support higher 11n rates
8 Value zero implies there is no restriction on maximum clients allowed.
9 MAC Filtering is not supported with FlexConnect Local authentication
10 MAC Filtering should be enabled.
11 Guest tunneling, Local switching, DHCP Required should be disabled.
12 Max-associated-clients feature and Central Assoc feature are not supported with FlexConnect Local Authentication.
13 VLAN based central switching is not supported with FlexConnect Local Authentication.
14 Enabling gtk-randomize will prevent clients from decrypting broadcast and multicast packets.
15 Fast Transition is supported with WPA2 and open security policy
16 Override Bandwidth Contracts parameters are specific to per Radio of AP. A value of zero (0) indicates that the value specified in the selected QoS profile will take effect.
18 When Diagnostic Channel is enabled, P2P Blocking Action will be assigned to Drop Action, L2 Security and L3 Security will be none
19 PMF should be disabled Before configuring 802.1x or CCKM or PSK.
20 This configuration override only Web Authentication Type and External Webauth URL. Redirect URL on global config always override the URL on each WLAN. Keep the configuration on global blank if you need per WLAN redirect.

5. On the shared services switch, add the following configuration to enable hairpin on the switch:

```
ip route-cache same-interface
```

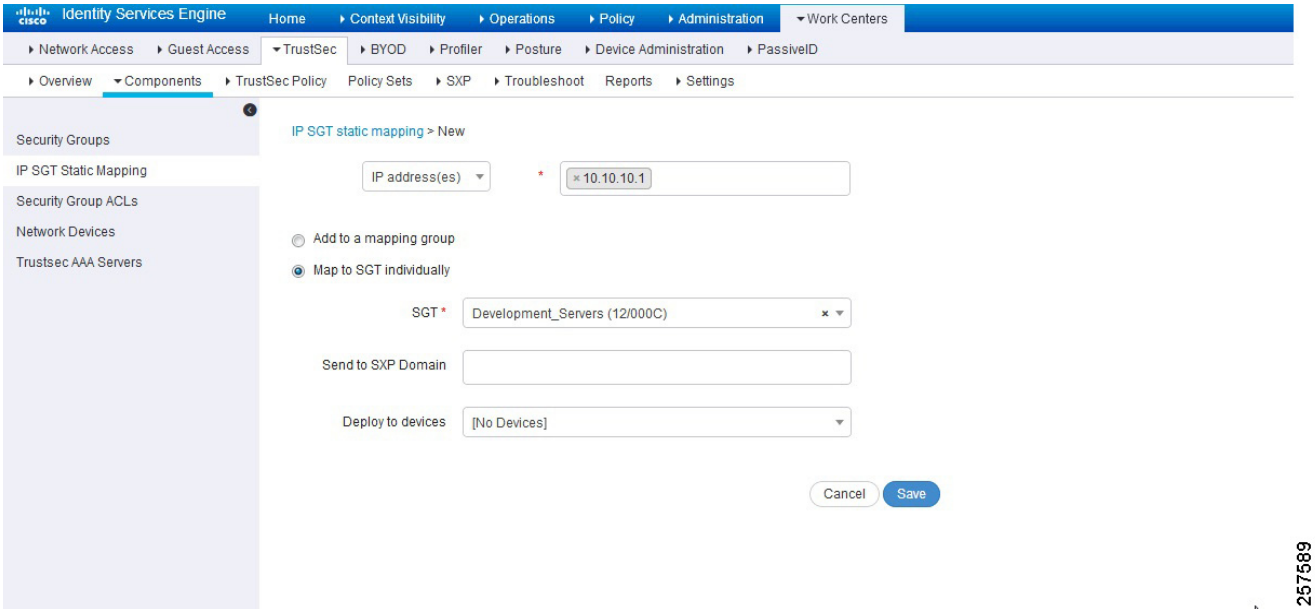
**Tip:** If this configuration is not added to the switch, all wireless to wireless traffic will be blocked since, by default, switches do not forward traffic to the source port.

## Static IP-SGT Mappings for Servers

Use IP to SGT static mapping on ISE to apply SGTs to traffic from the data center. To configure a new entry, follow these steps:

1. In **ISE**, navigate to **Work Centers > TrustSec > Components**.
2. Select **IP SGT Static Mapping** on the left panel.
3. Click **+Add**.
4. Add an IP address and select the radio button for **MAP to SGT Individually**. Select the **SGT** from the drop-down list.
5. From the **Deploy to Devices** drop-down list, select devices to map. Click **Save**.
6. Select the recently created entry from the list and click **Deploy**.
7. On the pop-up window, select devices to push the new mapping and apply configuration.

**Figure 26 IP to SGT Mapping**



IP address(es) *: 10.10.10.1

○ Add to a mapping group

● Map to SGT individually

SGT *: Development_Servers (12/000C)

Send to SXP Domain:

Deploy to devices: [No Devices]

# Visibility Configurations

In the Extended Enterprise design, the ISE profiling feature provides visibility and classification of the endpoints connected to the network. Using MAC addresses as the unique identifier for IoT endpoints that do not support 802.1x authentication, ISE collects various attributes for each network endpoint to build an internal endpoint database. ISE collects this information by different probes such as DHCP, HTTP, RADIUS, SNMP, Active Directory, NetFlow, DHCPSPAN, and Cisco Platform Exchange Grid (pxGrid). After collecting endpoint information, ISE begins the classification process.

The configuration process for ISE profiling begins with the enablement of specific probes on an ISE appliance configured as the PSN. Different probes are responsible for collecting different types of endpoint attributes. These attributes are matched to conditions that can then match rules across a library of device types, or profiles. Based on a generic weighting scale, each matching condition can be assigned a different weight, or certainty factor, that expresses the relative value that the condition contributes to classification of the device to a specific profile. Although conditions may match in multiple profiles, the profile for which the endpoint has the highest cumulative certainty factor, or total certainty factor, is the one assigned to the endpoint. This policy is referred to as the Matched Policy, or the Endpoint Profile Policy. Once profiled, the endpoint policy can be directly referenced in Authorization Policy Rule conditions.

The Extended Enterprise validation used out-of-the-box ISE configurations to profile IP cameras and IP phones. If customizing or creating an additional configuration is necessary, refer to the *ISE Profiling Design Guide* at the following URL:

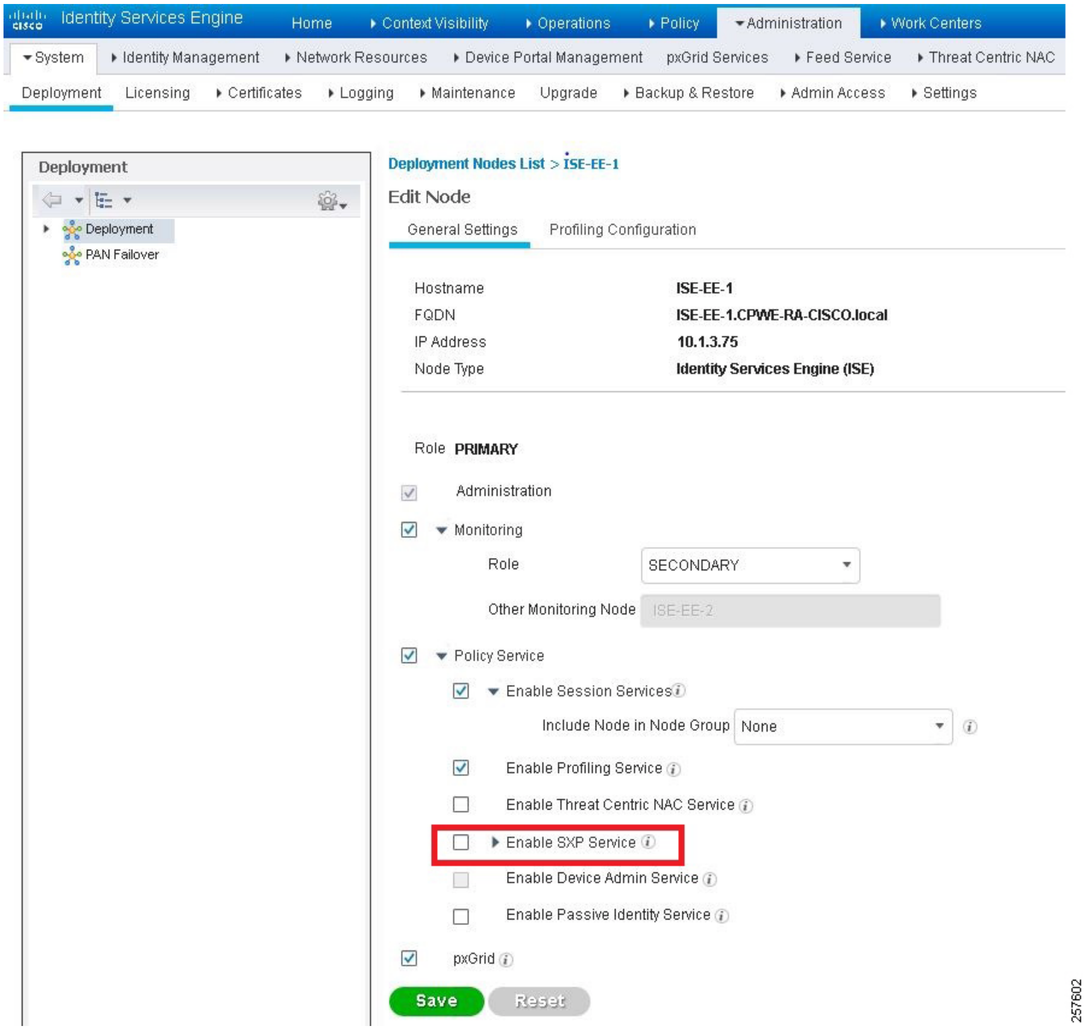
- https://community.cisco.com/t5/security-documents/ise-profiling-design-guide/ta-p/3739456

The following sections describe required configurations for endpoint profiling.

## Enable Profiling in Cisco ISE

1. Navigate to **Administration > System > Deployment**.
2. Select the node to be used for the profile service.
3. Check the **Enable Profiling Service** check box and then click **Save**.

**Figure 27 Enable ISE Profiling**



Hostname ISE-EE-1
FQDN ISE-EE-1.CPWE-RA-CISCO.local
IP Address 10.1.3.75
Node Type Identity Services Engine (ISE)

Role PRIMARY

☑ Administration
☑ Monitoring
Role SECONDARY
Other Monitoring Node ISE-EE-2
☑ Policy Service
☑ Enable Session Services
Include Node in Node Group None
☑ Enable Profiling Service
□ Enable Threat Centric NAC Service
□ Enable SXP Service
□ Enable Device Admin Service
□ Enable Passive Identity Service
☑ pxGrid

## Device Sensor Configuration in IE Switches

This section describes how to configure the device sensor so that it can be used for profiling purposes on ISE. The device sensor is a feature of access devices that collects information about connected endpoints. Information collected by the Device Sensor can come from the following protocols:

- Cisco Discovery Protocol (CDP)
- Link Layer Discovery Protocol (LLDP)
- Dynamic Host Configuration Protocol (DHCP)

**Tip:** Device sensor configuration can be pushed via template

1. (Optional) Configure filter lists and filter specs, which indicate the attributes that should be included in RADIUS accounting messages. The following example uses three filter lists for CDP, DHCP, and LLDP:

   ```
   Switch(config)#device-sensor filter-list cdp list iseCDP
    tlv name device-name
    tlv name capabilities-type
    tlv name version-type
    tlv name platform-type
   !
   device-sensor filter-list dhcp list iseDHCP
    option name host-name
    option name parameter-request-list
    option name class-identifier
   !
   device-sensor filter-list lldp list iseLLDP
    tlv name system-name
    tlv name system-description
    tlv name system-capabilities

   device-sensor filter-spec dhcp include list iseDHCP
   device-sensor filter-spec lldp include list iseLLDP
   device-sensor filter-spec cdp include list iseCDP
   ```

2. Add the following command to trigger updates whenever type, length, values (TLVs) are added, modified, or removed for the current session:

   ```
   Switch(config)#device-sensor notify all-changes
   ```

3. Configure accounting to send the information:

   ```
   Switch(config)#access-session attributes filter-list list Def_Acct_List
    cdp
    lldp
    dhcp
    http
   access-session accounting attributes filter-spec include list Def_Acct_List
   ```

4. Configure DHCP snooping to enable data collection from DHCP:

   ```
   Switch(config)#ip dhcp snooping
   ip dhcp snooping vlan $dhcp_snoop_vlans
   ```

# Security Troubleshooting

## SGT Classification

To ensure that an endpoint has received the correct SGT from Cisco ISE, log in to the ISE admin node:

1. Navigate to **Operations > Radius > Live Logs**. On the **Live Logs** page, filter for the endpoint in question. Live Log entries for the endpoint should be visible.

   Under the **Identity** column, #CTSREQUEST# appears any time SGT information is downloaded to the switch.

2. Click the **Details** icon for the log entry under the **Details** column. Near the bottom of the page in the **Results** section of the output, there are several entries for cisco-av-pairs. The av-pair: cts:security-group-tag=00-0000 contains the tag number issued to the endpoint.

Also, on the **Live Logs** page, SGT information can be found in the **Authorization Profiles** column. If the network device received SGT information along with the authorization profile for the endpoint, the name of the SGT will be displayed next to the **Authorization Profile** name.

To check the SGT to endpoint mapping for a port on the network device, issue the detailed **show access-session** command:

```
switch#show access-session interface interface detail
```

The section "Server Policies," which is near the end of the output, will have SGT information for the endpoint.

If the IP address of the endpoint is known, list all SGT to IP mappings on the switch and locate the endpoint IP:

```
switch#show cts role-based sgt-map all
```

## Device Sensor Troubleshooting

1. Verify switch connectivity with CDP and LLDP:

   ```
   switch#show cdp neighbors
   switch#show lldp neighbors
   ```

   If no information is displayed, check that the protocol is enabled with the command **sh running-config all | in cdp run**.

2. Check the device sensor cache:

   ```
   switch#show device-sensor cache interface g1/0/13
   ```

3. Verify attributes in RADIUS accounting by using the **debug radius** command on the switch or by performing a packet capture between the switch and ISE.

   An example of a relevant attribute to look for:

   ```
   Mar 30 05:34:58.716: RADIUS:   Cisco AVpair       [1]   34  "cdp-tlv=
   ```

4. Check the profiler debug logs in ISE. Enable profiler debugs for the correct PSN node at **Administration > System > Logging > Debug Log Configuration > PSN > Profiler > Debug** and re-attempt endpoint authentication.

## TrustSec Troubleshooting on ISE

#### Check SXP Mappings

Navigate to **Work Centers > TrustSec > SXP**. Select **All SXP Mappings** on the left panel. It will display all current mappings.

#### Check SXP Tunnels

Navigate to **Work Centers > TrustSec > SXP**. Select **SXP Devices** on the left panel. The **Status** column will show **ON** for the active tunnels.

## TrustSec Troubleshooting on the Enforcement Switch

### Check TrustSec Environment Data

The following switch command will display a list of SGTs configured in ISE. Make sure the current state is COMPLETE.

```
Switch#show cts environment-data
```

If the information is missing, run the **show cts pacs** command to see if the PAC was installed. If the PAC is not installed, the output will be empty. The **show cts server-list** command will display ISE information. If this information is not correct, make sure you have provisioned the device in the Cisco DNA Center as described in Provisioning Device in Inventory, page 21.

### Display Classification Entries in the Enforcement Switch

Use the following command to display IP-to-SGT mappings on the switch:

```
Switch#show cts role-based sgt-map all
```

## Endpoint Onboarding

At this point, the network is ready for endpoint onboarding, provided DHCP pools have been created for endpoints. You can connect endpoints to industrial switches or wirelessly to outdoor APs using the non-fabric SSID. The endpoint should receive the appropriate SGT and policies. If the endpoint is not able to connect, you can use the **Assurance Client Health** page to diagnose issues.

The following list provides a review of required configurations to help diagnose endpoint onboarding issues:

- There is a DHCP scope for endpoints and the **ip-helper address** command is configured.
- If the endpoint uses 802.1x authentication, the user should exist in the identity store configured in policy.
- If the endpoint is connecting with MAB authentication, and is not matching a profiling condition indicated in policy, check that correct attributes are being sent from the network device. Otherwise, it will use default authorization policy.
- For wireless endpoints, if the SSID is not available, verify that the WLC and APs were provisioned successfully.
- For wired endpoints, make sure the access switch port configuration has the correct port authentication and trunk settings.
- For wired endpoints, if device sensor is being used to send endpoint attributes, ensure the device sensor is configured correctly on the access switch.

# Assurance

Cisco DNA Center provides insights into enterprise networks by ingesting large amounts of data from network devices, clients, and sensors and analyzing data. Many key performance metrics are measured and correlated to focus on highlighting issues and providing guided solutions.

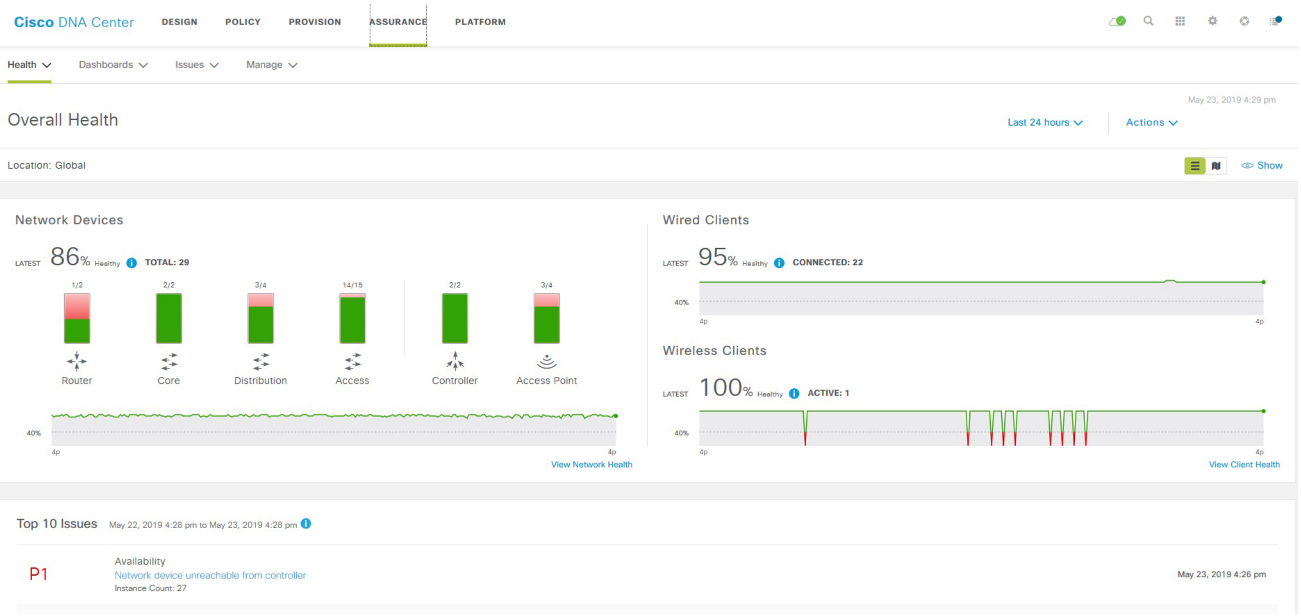
Network devices must be discovered, added to the inventory, and be in a managed state before the performance metrics of devices and clients can be viewed. Optionally, Assurance can integrate with ISE to provide more detail about connected clients. Various telemetry profiles can also be distributed to network devices to configure syslog, SNMP, and NetFlow.

## Overall Health

Navigate to **Assurance** from the **Cisco DNA Center** dashboard. **Assurance** displays the **Overall Health** page, which summarizes the health of the entire enterprise network using graphs to highlight network device and client health. The default view is 24 hours, but can be toggled between 3 hours, 24 hours, and 7 days using the **Last 24 hours** drop-down list near the top right of the page.

The **Show** toggle above the graphs can be used to turn the location pane on or off. This allows for listing devices and health status by site hierarchy, building, or geographic views. The **Top 10 Issues** pane follows the graphs of network device and client health. This pane aggregates and sorts issues by severity, giving a concise list of issues affecting the network with an instance count per issue.

**Figure 28 Assurance Dashboard**



P1 Availability
Network device unreachable from controller
Instance Count: 27
May 23, 2019 4:26 pm

257590

## Network Health

View a summary of network health by clicking **Health > Network** on the **Overall Health** page or by clicking **View Network Health** at the bottom right of the **Network Devices** graph.

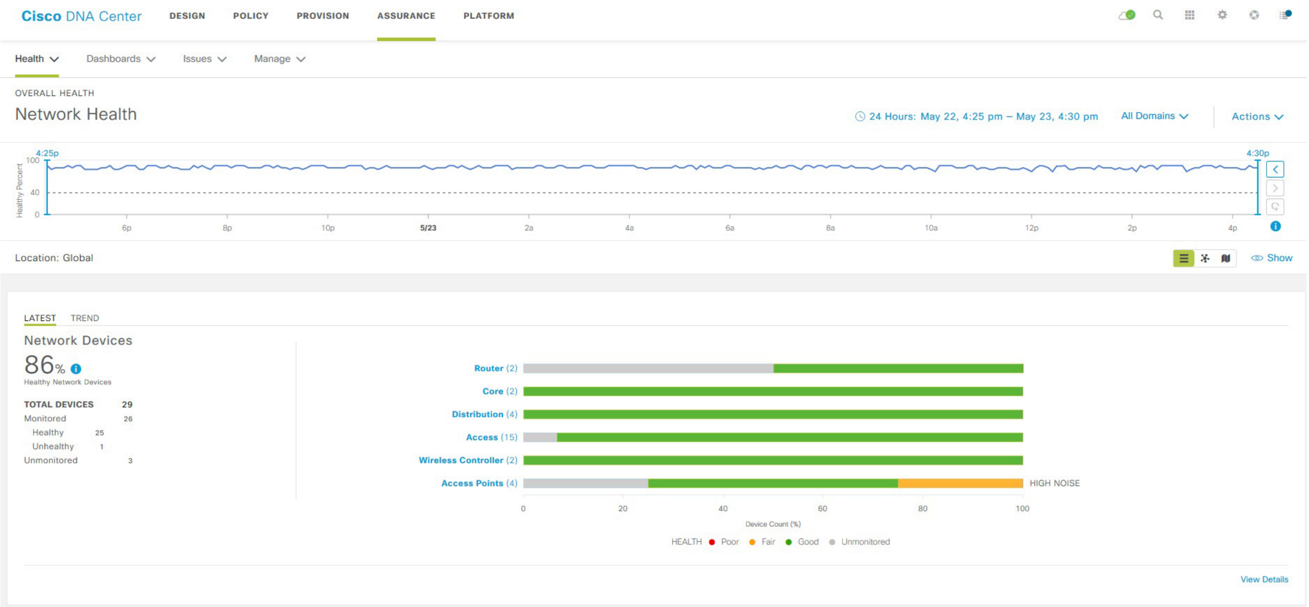
Near the top of the page, the network timeline is displayed. The slider bar can be adjusted to focus on a smaller slice of time. Using the **Last 24 Hours** drop-down list, up to 14 days of network health history are available.

In the **Network Devices** pane, devices are sorted by role and a summary of health score is indicated by color:

- **Red**–Critical issues. Health score range is 1 to 3.
- **Orange**–Warnings. Health score range is 4 to 7.
- **Green**–No errors or warning. Health score range is 8 to 10.
- **Gray**–No data available. Health score is 0.

Like the **Overall Health** page, the **Location** pane can be toggled on or off by clicking **Show**. This pane lists devices and health status by site hierarchy, building, topology, or geographic views.

## Figure 29 Network Health



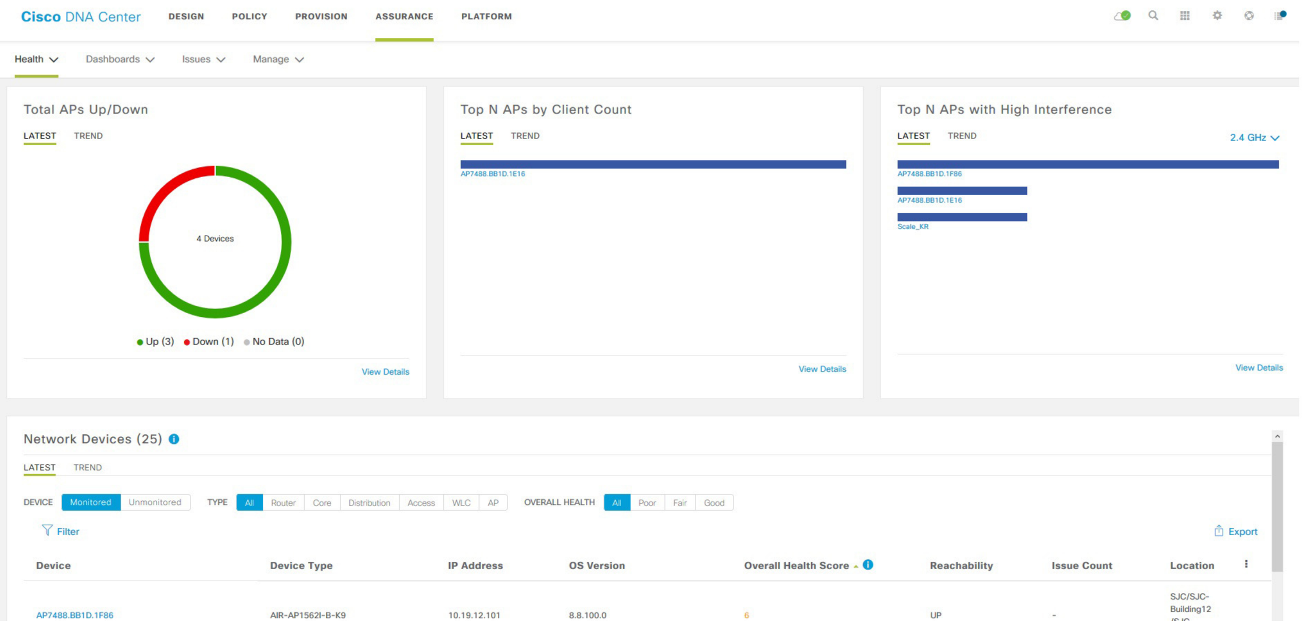
Network Devices

86% Healthy Network Devices

| | |
|---|---|
| TOTAL DEVICES | 29 |
| Monitored | 26 |
| Healthy | 25 |
| Unhealthy | 1 |
| Unmonitored | 3 |

Further down the **Network Health** page, panes display wireless AP information. Following the AP metrics is a **Network Devices** pane that lists all devices used to determine the network health metric.

## Figure 30 Wireless AP Health



| Device | Device Type | IP Address | OS Version | Overall Health Score | Reachability | Issue Count | Location |
|---|---|---|---|---|---|---|---|
| AP7488.BB1D.1F86 | AIR-AP1562I-B-K9 | 10.19.12.101 | 8.8.100.0 | 6 | UP | - | SJC/SJC-Building12 |

The list under **Network Devices** is filterable for quick identification of devices with outstanding issues. Hovering over the **Overall Health Score** for a given device will display the device health with health and percentage value of all KPI metrics. For more information about a device, click the device name to view complete information for the network device.

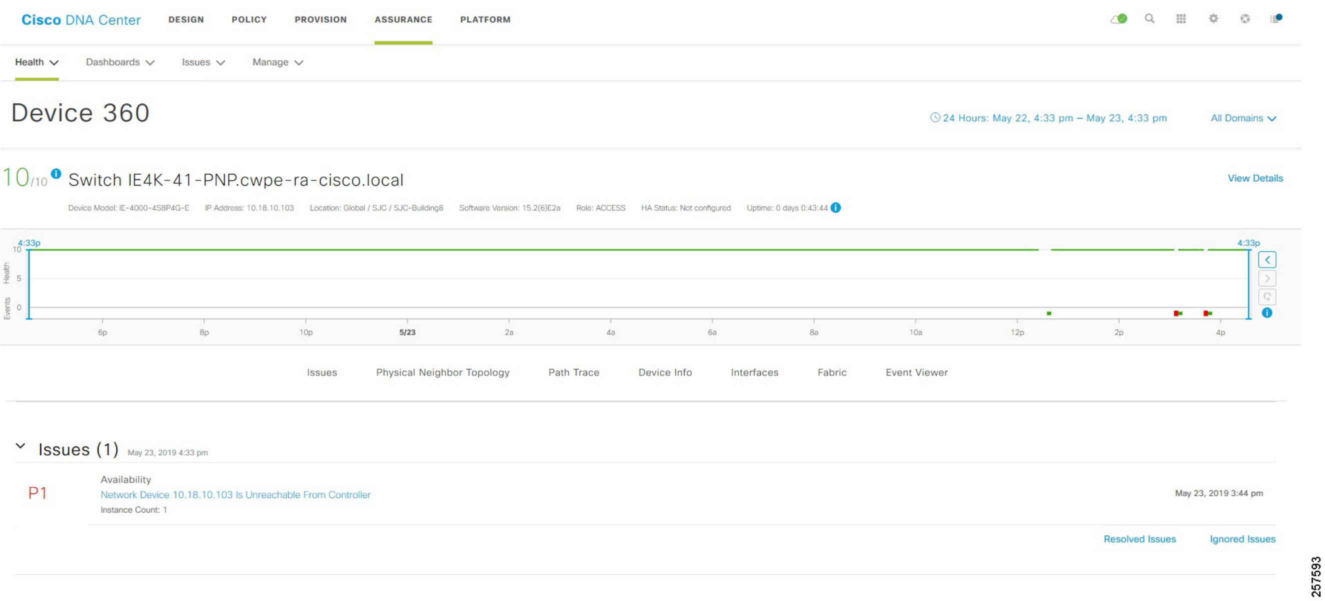
## Device 360

The **Device 360** page provides detailed information about a network device for troubleshooting issues.

At the top of the page, the **Historical Health Graph** displays device health over the specified time window. Click **View Details** in the upper right of the **Device 360** window to view network information and rack location.

The **Issues** pane lists any issues detected by DNA that should be corrected. The most recent issue is listed first. Click an issue to view details. Any issue remains in the open state until the status is changed by clicking **Status** and selecting **Ignore** or **Resolve**.

**Figure 31 Device 360**



Device 360

24 Hours: May 22, 4:33 pm – May 23, 4:33 pm    All Domains

10/10 Switch IE4K-41-PNP.cwpe-ra-cisco.local

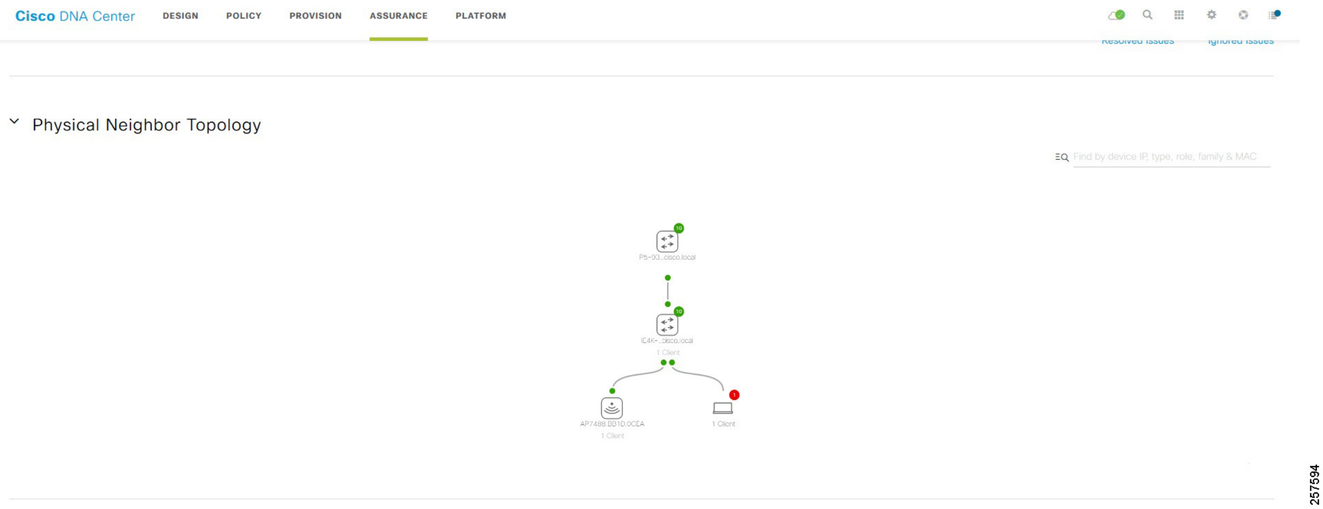
Device Model: IE-4000-4S8P4G-E    IP Address: 10.18.10.103    Location: Global / SJC / SJC-Building8    Software Version: 15.2(6)E2a    Role: ACCESS    HA Status: Not configured    Uptime: 0 days 0:43:44

Issues (1) May 23, 2019 4:33 pm

P1 Availability
Network Device 10.18.10.103 Is Unreachable From Controller
Instance Count: 1    May 23, 2019 3:44 pm

Following the **Issues** pane is the **Physical Neighbor Topology** pane. This shows connected devices and device and link health. Clicking a node brings up information about the target device. Hovering over a link displays details like interface numbers, admin status, and mode.

**Figure 32 Physical Network Topology**



Following the **Physical Neighbor Topology** is the **Event Viewer** pane. Event Viewer, which is for switches and routers, displays syslogs with a severity of **Error** or above. Link status and device reachability events are recorded here. For APs, scenarios and sub-events are listed to help determine during which sub-event an issue occurred.

**Warning:** On the **Device 360** page, you will find a **Path Trace** section. Path trace functionality is not described in this guide since in the Cisco DNA Center 1.2.10 release, this feature does not recognize extended nodes. Therefore, if a topology contains extended nodes, you may get an error message.

## Client Health

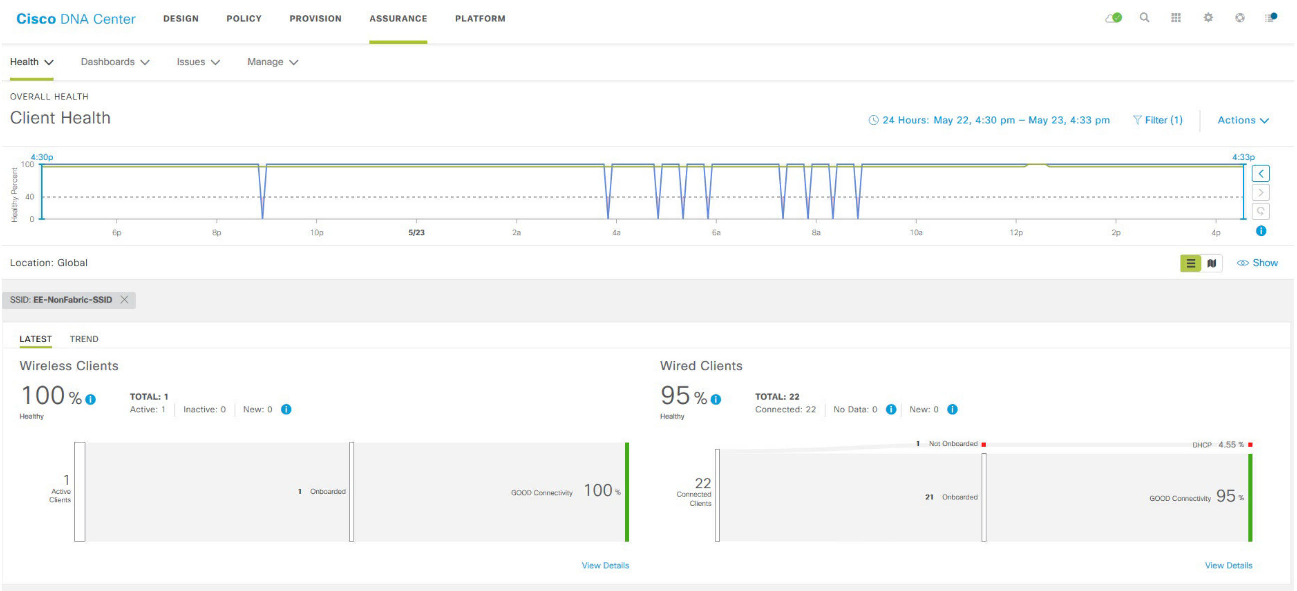
View a summary of client health by clicking **Health > Client** on the **Overall Health** screen or by clicking **View Client Health** at the bottom right of the **Wired and Wireless Clients** graph.

The client timeline is displayed near the top of the page. In the **Clients** pane, devices are sorted as **Wired** or **Wireless** clients, and a summary of health score is indicated by color.

- **Red**—Critical issues. Health score range is 1 to 3.
- **Orange**—Warnings. Health score range is 4 to 7.
- **Green**—No errors or warning. Health score range is 8 to 10.
- **Gray**—No data available. Health score is 0.

Like the **Overall Health** page, the **Location** pane can be toggled on or off by clicking **Show**. This pane lists client and health status by site hierarchy, building, topology, or geographic views.

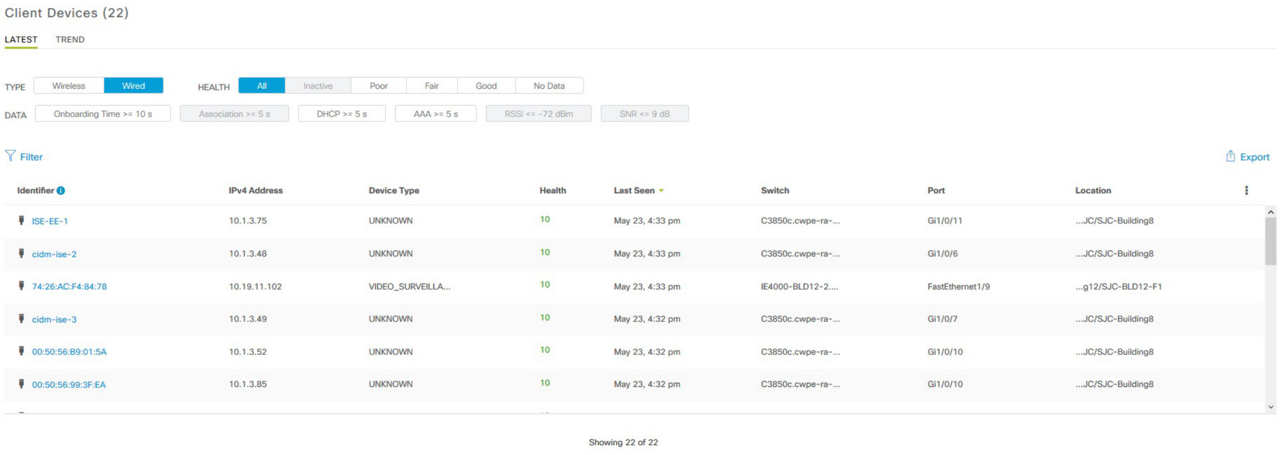
## Figure 33 Client Health



Further down the **Client Health** page, information is provided about Received Signal Strength Indication (RSSI), Signal-to-Noise Ratio (SNR), Roaming Times, Clients per SSID, Physical Link Connectivity, and Onboarding Times.

The **Client Devices** list is filterable for quick identification of clients with outstanding issues. The **Client Health** field displays the client health score, which is the average of its onboarding and connected scores. Health scores are calculated every five minutes. For more information about a client, click the client name to view Client 360 page for the device.

## Figure 34 Client Device List



| Identifier | IPv4 Address | Device Type | Health | Last Seen | Switch | Port | Location |
|---|---|---|---|---|---|---|---|
| ISE-EE-1 | 10.1.3.75 | UNKNOWN | 10 | May 23, 4:33 pm | C3850c.cwpe-ra-... | Gi1/0/11 | ...JC/SJC-Building8 |
| cidm-ise-2 | 10.1.3.48 | UNKNOWN | 10 | May 23, 4:33 pm | C3850c.cwpe-ra-... | Gi1/0/6 | ...JC/SJC-Building8 |
| 74:26:AC:F4:84:78 | 10.19.11.102 | VIDEO_SURVEILLA... | 10 | May 23, 4:33 pm | IE4000-BLD12-2.... | FastEthernet1/9 | ...g12/SJC-BLD12-F1 |
| cidm-ise-3 | 10.1.3.49 | UNKNOWN | 10 | May 23, 4:32 pm | C3850c.cwpe-ra-... | Gi1/0/7 | ...JC/SJC-Building8 |
| 00:50:56:B9:01:5A | 10.1.3.52 | UNKNOWN | 10 | May 23, 4:32 pm | C3850c.cwpe-ra-... | Gi1/0/10 | ...JC/SJC-Building8 |
| 00:50:56:99:3F:EA | 10.1.3.85 | UNKNOWN | 10 | May 23, 4:32 pm | C3850c.cwpe-ra-... | Gi1/0/10 | ...JC/SJC-Building8 |

Showing 22 of 22

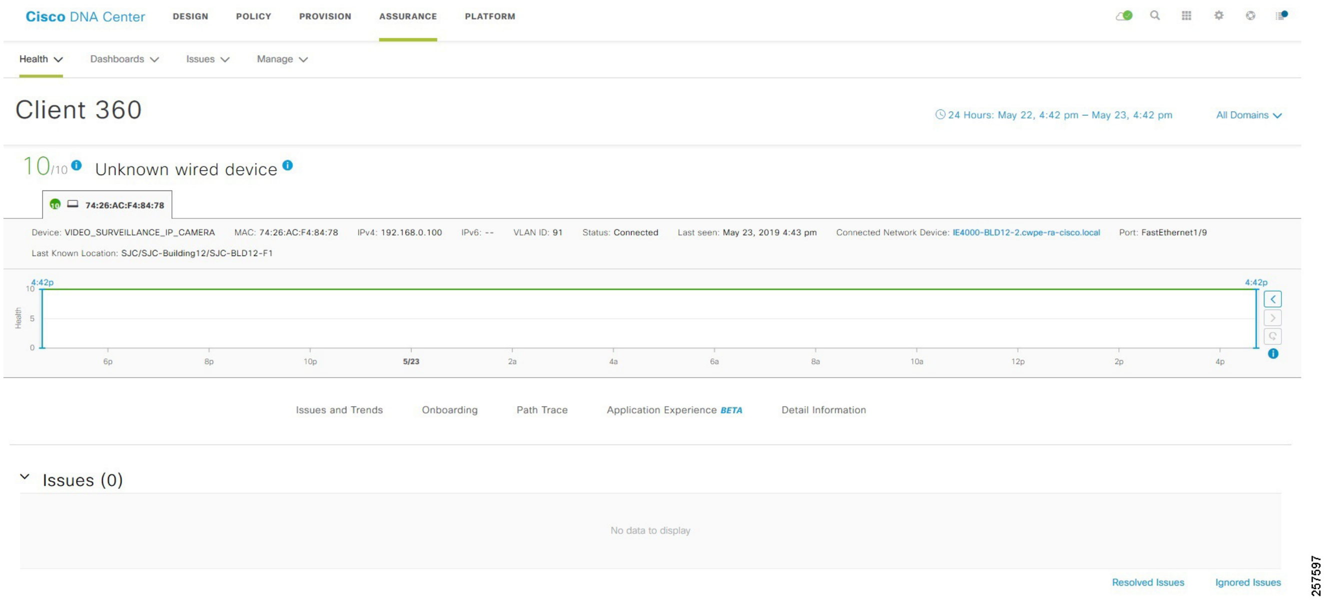
## Client 360

Client 360 provides detailed information about a client for troubleshooting issues.

At the top of the page, the **Historical Health Graph** displays device health for the past 24 hours. Using the **Last 24 Hours** drop-down list, this can be changed to 3 hours, 24 hours, or 7 days with a maximum history of 14 days.

The **Issues** pane lists any issues detected by Cisco DNA Center that should be corrected. The most recent issue is listed first. Click an issue to view details. Any issue remains in the open state until status is changed by clicking **Status** and then selecting **Ignore** or **Resolve**.

### Figure 35 Client 360



Client 360

24 Hours: May 22, 4:42 pm – May 23, 4:42 pm

10/10 Unknown wired device

74:26:AC:F4:84:78

Device: VIDEO_SURVEILLANCE_IP_CAMERA MAC: 74:26:AC:F4:84:78 IPv4: 192.168.0.100 IPv6: -- VLAN ID: 91 Status: Connected Last seen: May 23, 2019 4:43 pm Connected Network Device: IE4000-BLD12-2.cwpe-ra-cisco.local Port: FastEthernet1/9

Last Known Location: SJC/SJC-Building12/SJC-BLD12-F1

Issues (0)

No data to display

The **Onboarding** pane shows how the client connected to the network, information about onboarding services like DHCP and AAA, and device and link health. Clicking a node brings up information about the target device. Hovering over an endpoint displays details like interface numbers, admin status, and mode.

# Appendix A: Installation and Setup

## Cisco DNA Center Installation

Refer to the *CVD Software-Defined Access Deployment Guide* at the following URL:

- https://cvddocs.com/fw/251-prime

For a more detailed setup of the appliance specific to chassis type, refer to Install and Upgrade Guides at the following URL:

- https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-installation-guides-list.html

## ISE and WLC Installation and Integration

Refer to the *CVD Software-Defined Access Deployment Guide* at the following URL:

- https://cvddocs.com/fw/251-prime

# Appendix B: Sample Template used in CVD Verification

## Sample Device Sensor Configuration

```
ip dhcp snooping
ip dhcp snooping vlan $dhcp_snoop_vlans
access-session attributes filter-list list Def_Acct_List
 cdp
 lldp
 dhcp
 http
access-session accounting attributes filter-spec include list Def_Acct_List

device-sensor filter-list cdp list iseCDP
 tlv name device-name
 tlv name capabilities-type
 tlv name version-type
 tlv name platform-type
!
device-sensor filter-list dhcp list iseDHCP
 option name host-name
 option name parameter-request-list
 option name class-identifier
!
device-sensor filter-list lldp list iseLLDP
 tlv name system-name
 tlv name system-description
 tlv name system-capabilities
device-sensor filter-spec dhcp include list iseDHCP
device-sensor filter-spec lldp include list iseLLDP
device-sensor filter-spec cdp include list iseCDP
device-sensor notify all-changes
```

## Sample AAA Policies

```
class-map type control subscriber match-all AAA_SVR_DOWN_AUTHD_HOST
 match authorization-status authorized
 match result-type aaa-timeout
!
class-map type control subscriber match-all AAA_SVR_DOWN_UNAUTHD_HOST
 match authorization-status unauthorized
 match result-type aaa-timeout
!
class-map type control subscriber match-all AUTHC_SUCCESS-AUTHZ_FAIL
 match authorization-status unauthorized
 match result-type success
!
class-map type control subscriber match-all DOT1X
 match method dot1x
!
class-map type control subscriber match-all DOT1X_FAILED
 match method dot1x
 match result-type method dot1x authoritative
!
class-map type control subscriber match-all DOT1X_MEDIUM_PRIO
 match authorizing-method-priority gt 20
!
class-map type control subscriber match-all DOT1X_NO_RESP
 match method dot1x
 match result-type method dot1x agent-not-found
!
class-map type control subscriber match-all DOT1X_TIMEOUT
 match method dot1x
 match result-type method dot1x method-timeout
 match result-type method-timeout
!
class-map type control subscriber match-any IN_CRITICAL_AUTH
 match activated-service-template DefaultCriticalVoice_SRV_TEMPLATE
!
class-map type control subscriber match-any IN_CRITICAL_AUTH_CLOSED_MODE
 match activated-service-template DefaultCriticalAuthVlan_SRV_TEMPLATE
 match activated-service-template DefaultCriticalVoice_SRV_TEMPLATE
!
class-map type control subscriber match-all MAB
 match method mab
!
class-map type control subscriber match-all MAB_FAILED
 match method mab
 match result-type method mab authoritative
!
class-map type control subscriber match-none NOT_IN_CRITICAL_AUTH
 match activated-service-template DefaultCriticalVoice_SRV_TEMPLATE
!
class-map type control subscriber match-none NOT_IN_CRITICAL_AUTH_CLOSED_MODE
 match activated-service-template DefaultCriticalAuthVlan_SRV_TEMPLATE
 match activated-service-template DefaultCriticalVoice_SRV_TEMPLATE
!
!
!
policy-map type control subscriber PMAP_DefaultWiredDot1xClosedAuth_1X_MAB
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority 10
 event authentication-failure match-first
  5 class DOT1X_FAILED do-until-failure
```

```
   10 terminate dot1x
   20 authenticate using mab priority 20
  10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
   10 activate service-template DefaultCriticalAuthVlan_SRV_TEMPLATE
   20 activate service-template DefaultCriticalVoice_SRV_TEMPLATE
   30 authorize
   40 pause reauthentication
  20 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
   10 pause reauthentication
   20 authorize
  30 class DOT1X_NO_RESP do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  40 class MAB_FAILED do-until-failure
   10 terminate mab
   20 authentication-restart 60
  60 class always do-until-failure
   10 terminate dot1x
   20 terminate mab
   30 authentication-restart 60
 event aaa-available match-all
  10 class IN_CRITICAL_AUTH_CLOSED_MODE do-until-failure
   10 clear-session
  20 class NOT_IN_CRITICAL_AUTH_CLOSED_MODE do-until-failure
   10 resume reauthentication
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x retries 2 retry-time 0 priority 10
 event inactivity-timeout match-all
  10 class always do-until-failure
   10 clear-session
 event authentication-success match-all
 event violation match-all
  10 class always do-until-failure
   10 restrict
 event authorization-failure match-all
  10 class AUTHC_SUCCESS-AUTHZ_FAIL do-until-failure
   10 authentication-restart 60
!
policy-map type control subscriber PMAP_DefaultWiredDot1xClosedAuth_MAB_1X
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using mab priority 20
 event authentication-failure match-first
  5 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authentication-restart 60
  10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
   10 activate service-template DefaultCriticalAuthVlan_SRV_TEMPLATE
   20 activate service-template DefaultCriticalVoice_SRV_TEMPLATE
   30 authorize
   40 pause reauthentication
  20 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
   10 pause reauthentication
   20 authorize
  30 class MAB_FAILED do-until-failure
   10 terminate mab
   20 authenticate using dot1x retries 2 retry-time 0 priority 10
  40 class DOT1X_NO_RESP do-until-failure
   10 terminate dot1x
   20 authentication-restart 60
  60 class always do-until-failure
   10 terminate mab
   20 terminate dot1x
   30 authentication-restart 60
 event aaa-available match-all
  10 class IN_CRITICAL_AUTH_CLOSED_MODE do-until-failure
   10 clear-session
  20 class NOT_IN_CRITICAL_AUTH_CLOSED_MODE do-until-failure
   10 resume reauthentication
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x retries 2 retry-time 0 priority 10
 event inactivity-timeout match-all
  10 class always do-until-failure
   10 clear-session
 event authentication-success match-all
 event violation match-all
  10 class always do-until-failure
   10 restrict
 event authorization-failure match-all
  10 class AUTHC_SUCCESS-AUTHZ_FAIL do-until-failure
   10 authentication-restart 60
!
policy-map type control subscriber PMAP_DefaultWiredDot1xLowImpactAuth_1X_MAB
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority 10
 event authentication-failure match-first
  5 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
   10 activate service-template DefaultCriticalAuthVlan_SRV_TEMPLATE
   20 activate service-template DefaultCriticalVoice_SRV_TEMPLATE
   25 activate service-template DefaultCriticalAccess_SRV_TEMPLATE
   30 authorize
   40 pause reauthentication
  20 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
   10 pause reauthentication
   20 authorize
  30 class DOT1X_NO_RESP do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  40 class MAB_FAILED do-until-failure
   10 terminate mab
   20 authentication-restart 60
  60 class always do-until-failure
   10 terminate dot1x
   20 terminate mab
   30 authentication-restart 60
 event aaa-available match-all
  10 class IN_CRITICAL_AUTH do-until-failure
   10 clear-session
  20 class NOT_IN_CRITICAL_AUTH do-until-failure
   10 resume reauthentication
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x retries 2 retry-time 0 priority 10
 event inactivity-timeout match-all
  10 class always do-until-failure
   10 clear-session
 event authentication-success match-all
 event violation match-all
  10 class always do-until-failure
```

```
   10 restrict
 event authorization-failure match-all
  10 class AUTHC_SUCCESS-AUTHZ_FAIL do-until-failure
   10 authentication-restart 60
!
policy-map type control subscriber PMAP_DefaultWiredDot1xLowImpactAuth_MAB_1X
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using mab priority 20
 event authentication-failure match-first
  5 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authentication-restart 60
  10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
   10 activate service-template DefaultCriticalAuthVlan_SRV_TEMPLATE
   20 activate service-template DefaultCriticalVoice_SRV_TEMPLATE
   25 activate service-template DefaultCriticalAccess_SRV_TEMPLATE
   30 authorize
   40 pause reauthentication
  20 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
   10 pause reauthentication
   20 authorize
  30 class MAB_FAILED do-until-failure
   10 terminate mab
   20 authenticate using dot1x retries 2 retry-time 0 priority 10
  40 class DOT1X_NO_RESP do-until-failure
   10 terminate dot1x
   20 authentication-restart 60
  60 class always do-until-failure
   10 terminate mab
   20 terminate dot1x
   30 authentication-restart 60
 event aaa-available match-all
  10 class IN_CRITICAL_AUTH do-until-failure
   10 clear-session
  20 class NOT_IN_CRITICAL_AUTH do-until-failure
   10 resume reauthentication
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x retries 2 retry-time 0 priority 10
 event inactivity-timeout match-all
  10 class always do-until-failure
   10 clear-session
 event authentication-success match-all
 event violation match-all
  10 class always do-until-failure
   10 restrict
 event authorization-failure match-all
  10 class AUTHC_SUCCESS-AUTHZ_FAIL do-until-failure
   10 authentication-restart 60
!
policy-map type control subscriber PMAP_DefaultWiredDot1xOpenAuth_1X_MAB
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority 10
 event authentication-failure match-first
  5 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
   10 activate service-template DefaultCriticalAuthVlan_SRV_TEMPLATE
   20 activate service-template DefaultCriticalVoice_SRV_TEMPLATE
   30 authorize
   40 pause reauthentication
  20 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
   10 pause reauthentication
   20 authorize
  30 class DOT1X_NO_RESP do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  40 class MAB_FAILED do-until-failure
   10 terminate mab
   20 authentication-restart 60
  60 class always do-until-failure
   10 terminate dot1x
   20 terminate mab
   30 authentication-restart 60
 event aaa-available match-all
  10 class IN_CRITICAL_AUTH do-until-failure
   10 clear-session
  20 class NOT_IN_CRITICAL_AUTH do-until-failure
   10 resume reauthentication
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x retries 2 retry-time 0 priority 10
 event inactivity-timeout match-all
  10 class always do-until-failure
   10 clear-session
 event authentication-success match-all
 event violation match-all
  10 class always do-until-failure
   10 restrict
 event authorization-failure match-all
  10 class AUTHC_SUCCESS-AUTHZ_FAIL do-until-failure
   10 authentication-restart 60
!
policy-map type control subscriber PMAP_DefaultWiredDot1xOpenAuth_MAB_1X
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using mab priority 20
 event authentication-failure match-first
  5 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authentication-restart 60
  10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
   10 activate service-template DefaultCriticalAuthVlan_SRV_TEMPLATE
   20 activate service-template DefaultCriticalVoice_SRV_TEMPLATE
   30 authorize
   40 pause reauthentication
  20 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
   10 pause reauthentication
   20 authorize
  30 class MAB_FAILED do-until-failure
   10 terminate mab
   20 authenticate using dot1x retries 2 retry-time 0 priority 10
  40 class DOT1X_NO_RESP do-until-failure
   10 terminate dot1x
   20 authentication-restart 60
  60 class always do-until-failure
   10 terminate mab
   20 terminate dot1x
   30 authentication-restart 60
 event aaa-available match-all
  10 class IN_CRITICAL_AUTH do-until-failure
   10 clear-session
  20 class NOT_IN_CRITICAL_AUTH do-until-failure
```

```
   10 resume reauthentication
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x retries 2 retry-time 0 priority 10
 event inactivity-timeout match-all
  10 class always do-until-failure
   10 clear-session
 event authentication-success match-all
 event violation match-all
  10 class always do-until-failure
   10 restrict
 event authorization-failure match-all
  10 class AUTHC_SUCCESS-AUTHZ_FAIL do-until-failure
   10 authentication-restart 60
```

## Sample Onboarding Configuration

```
hostname $hostname

vlan 90-95
!
interface Port-channel1
 switchport trunk allowed vlan 1,90-95
 switchport mode dynamic desirable
 no port-channel standalone-disable
!
interface range GigabitEthernet1/1-2
 switchport trunk allowed vlan 1,90-95
 switchport mode dynamic desirable
 channel-protocol lacp
 channel-group 1 mode active
!
ip default-gateway 10.19.10.1
!
ip http server
ip http secure-server
ip http client source-interface Vlan90
ip ssh source-interface Vlan90
ip ssh version 2


ntp server 10.13.15.241

line con 0
  logging synchronous
line vty 0 4
 exec-timeout 0 0
 privilege level 15
 transport preferred none
 transport input ssh
line vty 5 15
!
epm logging

end
```

## Sample Interface Configuration

```
#macro(AP_interface)
 switchport access vlan 92
 switchport mode access
#end

#macro(IP_Phones_interface)
 switchport voice vlan 93
 switchport access vlan 94
 switchport mode access
 authentication periodic
 authentication timer reauthenticate server
 access-session closed
 access-session port-control auto
 mab
 dot1x pae authenticator
 service-policy type control subscriber PMAP_DefaultWiredDot1xClosedAuth_MAB_1X
#end


#if ($AP_interface != "" )
    interface $AP_interface
    #AP_interface
#end

#if ($IP_Phone_interface != "" )
    interface $IP_Phone_interface
    #IP_Phones_interface
#end
```