Networking and Security in Industrial Automation Environments

Configuring the Infrastructure

Switch Configuration

The following configuration tools are used in this guide for configuration and management of Cisco IE switches:

- Device Manager
- Cisco IOS Command Line Interface (CLI)
- IND Plug-and-Play

Device Manager

You can use Device Manager, which is in the switch memory, to manage individual switches. This web interface offers quick configuration and monitoring. You can access Device Manager from anywhere in your network through a web browser. For more information, see the Device Manager online help.

Some of the features that can be configured with Device Manage are:

- Port settings
- Etherchannels
- Resilient Ethernet Protocol (REP)
- Smartport
- Spanning Tree Protocol (STP)
- VLAN
- VLAN Trunking Protocol (VTP)
- Authentication, Authorization, and Accounting (AAA)
- Multicast
- Quality of Service (QoS)

The following sections contain some features that are configured using device manager. For a complete list and configuration details and options, see the Device Manager online help.

Traffic Segmentation

- VLAN in **Configuration ->Layer 2 -> VLAN**

Interface Configurations

- Switch virtual interfaces (SVIs) in **Configuration -> Layer 2 -> VLAN**
- Interface settings in **Configuration -> Interface -> Ethernet**
- EtherChannel in **Configuration -> Interface -> Logical**

Redundancy

- Etherchannel in **Configuration -> Interface -> Logical**
- REP in **Configuration -> Layer 2 -> REP**

Routing

- Default Gateway in **Configuration -> Routing Protocols -> Static Routing**
- Static routes in **Configuration -> Routing Protocols -> Static Routing**

Security

- Access control lists (ACLs) in **Configuration -> Security -> ACL**
- AAA in **Configuration -> Security -> AAA**
- User creation in **Administration -> Management -> User Administration**

Other Configuration

- VTP in **Configuration -> Layer 2 -> VTP**
- Interface Smartport macros in **Configuration -> Layer 2 -> Smartports**
- IGMP snooping in **Configuration -> Services -> Multicast**
- QoS in **Configuration -> Services -> Multicast**
- PTP in **Administration -> Management -> Time**
- Network Time Protocol (NTP) in **Administration -> Management -> Time**
- CIP in **Administration -> Management -> CIP**

Command Line Interface

The switch CLI is based on Cisco IOS software and is enhanced to support desktop-switching features. You can fully configure and monitor the switch. You can access the CLI either by connecting your management station directly to the switch management port, connecting to a console port, or by using Telnet or SSH from a remote management station.

The following sections contain some configurations that are not possible using Device Manager and should be configured using CLI.

Line Passwords Encryption

The password encryption service is enabled in the global configuration with the following command:

```
service password-encryption
```

Logging Settings

To configure the logging buffer size or the time stamping service:

```
logging buffered 16384
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
```

Error Disable

To fully configure the error-disable feature, use the following commands:

```
errdisable recovery cause udld
errdisable recovery cause bpduguard
errdisable recovery cause security-violation
errdisable recovery cause channel-misconfig
errdisable recovery cause pagp-flap
errdisable recovery cause dtp-flap
errdisable recovery cause link-flap
errdisable recovery cause sfp-config-mismatch
errdisable recovery cause gbic-invalid
errdisable recovery cause psecure-violation
errdisable recovery cause port-mode-failure
errdisable recovery cause dhcp-rate-limit
errdisable recovery cause mac-limit
errdisable recovery cause vmps
errdisable recovery cause storm-control
errdisable recovery cause arp-inspection
errdisable recovery cause loopback
errdisable recovery interval 30
```

VTY Line Configuration

If desired the VTY lines must be configured to use SSH only. By default they accept both SSH and Telnet. Add the following configuration under line settings:

```
transport input ssh
```

Smartport

Smartport macros provide a convenient way to save and share common configurations. You can use Smartport macros to enable features and settings based on the location of a switch in the network and for mass configuration deployments across the network.

Each Smartport macro is a set of CLI commands that you define. Smartport macros do not contain new CLI commands; they are simply a group of existing CLI commands.

When you apply a Smartport macro to an interface, the CLI commands within the macro are configured on the interface. When the macro is applied to an interface, the existing interface configurations are not lost. The new commands are added to the interface and are saved in the running configuration file.

Refer to Cisco Industrial Ethernet 4000, 4010 and 5000 Switch Software Configuration Guide for Smartport configuration details:
https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie4010/software/release/15-2_4_EC/configuration/guide/scg-ie4010_5000/swmacro.html

Smartport Examples

After running the express setup you could apply the following configuration macros through the CLI:

cisco-global

The cisco-global macro applies the following configurations:

- Enable dynamic port error recovery for link state failures.
- Enable aggressive mode UniDirectional Link Detection (UDLD) on all fiber uplinks.
- Enable Rapid Per VLAN Spanning Tree Plus (Rapid PVST+) and Loopguard.

To apply use the following command in configuration mode:

```
macro global apply cisco-global
```

cisco-ie-global

The cisco-ie-global macro applies the following configurations:

- Access list and policy map for Common Industrial Protocol (CIP) QoS.
- Configures IP Internet Group Management Protocol (IGM) snooping and IP IGMP snooping querier.
- Configures spanning-tree mode to MST and Loopguard.

To apply use the following command in configuration mode:

```
macro global apply cisco-ie-global
```

QoS Configuration Examples

Cisco IE 2000:

```
!
access-list 101 permit udp any eq 2222 any dscp 55
access-list 102 permit udp any eq 2222 any dscp 47
access-list 103 permit udp any eq 2222 any dscp 43
access-list 104 permit udp any eq 2222 any
access-list 105 permit udp any eq 44818 any
access-list 105 permit tcp any eq 44818 any
access-list 106 permit udp any eq 319 any
access-list 107 permit udp any eq 320 any
!
policy-map CIP-PTP-Traffic
 class CIP-Implicit_dscp_55
  set qos-group 1
 class CIP-Implicit_dscp_47
  set qos-group 1
 class CIP-Implicit_dscp_43
  set qos-group 1
 class CIP-Implicit_dscp_any
  set qos-group 2
 class CIP-Other
  set qos-group 2
 class 1588-PTP-Event
  set qos-group 0
 class 1588-PTP-General
  set qos-group 1
!
class-map match-all 1588-PTP-General
 match access-group 107
class-map match-all 1588-PTP-Event
 match access-group 106
class-map match-all CIP-Other
 match access-group 105
class-map match-all CIP-Implicit_dscp_any
 match access-group 104
class-map match-all CIP-Implicit_dscp_43
```

```
 match access-group 103
class-map match-all CIP-Implicit_dscp_47
 match access-group 102
class-map match-all CIP-Implicit_dscp_55
 match access-group 101
!
!!! cisco-ie-qos-map-setup !!!
!
mls qos map policed-dscp 24 27 31 43 46 47 55 59 to 0
mls qos map cos-dscp 0 8 16 27 32 47 55 59
mls qos srr-queue input threshold 1 16 66
mls qos srr-queue input threshold 2 34 66
mls qos srr-queue input buffers 40 60
mls qos srr-queue input bandwidth 40 60
mls qos map dscp-cos 0 1 2 3 4 5 6 7 to 0
mls qos map dscp-cos 9 11 12 13 14 15 to 0
mls qos map dscp-cos 8 10 to 1
mls qos map dscp-cos 16 17 18 19 20 21 22 23 to 2
mls qos map dscp-cos 25 26 28 29 30 to 2
mls qos map dscp-cos 24 27 31 to 3
mls qos map dscp-cos 32 33 34 35 36 37 38 39 to 4
mls qos map dscp-cos 40 41 42 44 45 49 to 4
mls qos map dscp-cos 50 51 52 53 54 56 57 58 to 4
mls qos map dscp-cos 60 61 62 63 to 4
mls qos map dscp-cos 43 46 47 to 5
mls qos map dscp-cos 48 55 to 6
mls qos map dscp-cos 59 to 7
no mls qos rewrite ip dscp
# Return the egress queue-set configurations to default
no mls qos queue-set output 1 threshold 2
```

Cisco IE 4000:

```
!
access-list 101 permit udp any eq 2222 any dscp 55
access-list 102 permit udp any eq 2222 any dscp 47
access-list 103 permit udp any eq 2222 any dscp 43
access-list 104 permit udp any eq 2222 any
access-list 105 permit udp any eq 44818 any
access-list 105 permit tcp any eq 44818 any
access-list 106 permit udp any eq 319 any
access-list 107 permit udp any eq 320 any
!
policy-map CIP-PTP-Traffic
 class CIP-Implicit_dscp_55
  set qos-group 1
 class CIP-Implicit_dscp_47
  set qos-group 1
 class CIP-Implicit_dscp_43
  set qos-group 1
 class CIP-Implicit_dscp_any
  set qos-group 2
 class CIP-Other
  set qos-group 2
 class 1588-PTP-Event
  set qos-group 0
 class 1588-PTP-General
  set qos-group 1
!
policy-map PTP-Event-Priority
 class qos-group-0
  priority
```

```
 class qos-group-1
  bandwidth remaining percent 40
 class qos-group-2
  bandwidth remaining percent 40
 class class-default
  bandwidth remaining percent 20
!
class-map match-all 1588-PTP-General
 match access-group 107
class-map match-all 1588-PTP-Event
 match access-group 106
class-map match-all CIP-Other
 match access-group 105
class-map match-all CIP-Implicit_dscp_any
 match access-group 104
class-map match-all CIP-Implicit_dscp_43
 match access-group 103
class-map match-all CIP-Implicit_dscp_47
 match access-group 102
class-map match-all CIP-Implicit_dscp_55
 match access-group 101
!
class-map match-all qos-group-2
 match qos-group 2
class-map match-all qos-group-1
 match qos-group 1
class-map match-all qos-group-0
 match qos-group 0
!
```

Cisco IE 3X00

```
!
access-list 101 permit udp any eq 2222 any dscp 55
access-list 102 permit udp any eq 2222 any dscp 47
access-list 103 permit udp any eq 2222 any dscp 43
access-list 104 permit udp any eq 2222 any
access-list 105 permit udp any eq 44818 any
access-list 105 permit tcp any eq 44818 any
access-list 106 permit udp any eq 319 any
access-list 107 permit udp any eq 320 any
!
policy-map CIP-PTP-Traffic
 class CIP-Implicit_dscp_55
  set ip dscp 55
 class CIP-Implicit_dscp_47
  set ip dscp 47
 class CIP-Implicit_dscp_43
  set ip dscp 43
 class CIP-Implicit_dscp_any
  set ip dscp 31
 class CIP-Other
  set ip dscp 27
 class 1588-PTP-Event
  set ip dscp 59
 class 1588-PTP-General
  set ip dscp 47
!
policy-map PTP-Event-Priority
  class class-0
    priority
  class class-1
    bandwidth remaining percent 40
  class class-2
```

```
    bandwidth remaining percent 20
  class class-default
    bandwidth remaining percent 40
!
class-map match-all 1588-PTP-General
  match access-group 107
class-map match-all 1588-PTP-Event
  match access-group 106
class-map match-all CIP-Other
 match access-group 105
class-map match-all CIP-Implicit_dscp_any
 match access-group 104
class-map match-all CIP-Implicit_dscp_43
 match access-group 103
class-map match-all CIP-Implicit_dscp_47
 match access-group 102
class-map match-all CIP-Implicit_dscp_55
 match access-group 101
!
class-map match-all class-2
  match ip dscp ef
class-map match-all class-1
  match ip dscp 47
class-map match-all class-0
  match ip dscp 59
!
```

Cisco Catalyst 3850:

```
!
access-list 101 permit udp any eq 2222 any dscp 55
access-list 102 permit udp any eq 2222 any dscp 47
access-list 103 permit udp any eq 2222 any dscp 43
access-list 104 permit udp any eq 2222 any
access-list 105 permit udp any eq 44818 any
access-list 105 permit tcp any eq 44818 any
access-list 106 permit udp any eq 319 any
access-list 107 permit udp any eq 320 any
!
policy-map CIP-PTP-Traffic
 class CIP-Implicit_dscp_55
  set qos-group 1
 class CIP-Implicit_dscp_47
  set qos-group 1
 class CIP-Implicit_dscp_43
  set qos-group 1
 class CIP-Implicit_dscp_any
  set qos-group 2
 class CIP-Other
  set qos-group 2
 class 1588-PTP-Event
  set qos-group 0
 class 1588-PTP-General
  set qos-group 1
!
policy-map PTP-Event-Priority
 class qos-group-0
  priority level 1
 class qos-group-1
  bandwidth remaining percent 40
 class qos-group-2
  bandwidth remaining percent 40
```

```
 class class-default
  bandwidth remaining percent 20
!
class-map match-any 1588-PTP-General
 match access-group 107
class-map match-any 1588-PTP-Event
 match access-group 106
class-map match-any CIP-Other
 match access-group 105
class-map match-any CIP-Implicit_dscp_any
 match access-group 104
class-map match-any CIP-Implicit_dscp_43
 match access-group 103
class-map match-any CIP-Implicit_dscp_47
 match access-group 102
class-map match-any CIP-Implicit_dscp_55
 match access-group 101
!
class-map match-any qos-group-2
 match qos-group 2
class-map match-any qos-group-1
 match qos-group 1
class-map match-any qos-group-0
 match qos-group 0
!
```

Cisco Catalyst 9300:

```
!
access-list 101 permit udp any eq 2222 any dscp 55
access-list 102 permit udp any eq 2222 any dscp 47
access-list 103 permit udp any eq 2222 any dscp 43
access-list 104 permit udp any eq 2222 any
access-list 105 permit udp any eq 44818 any
access-list 105 permit tcp any eq 44818 any
access-list 106 permit udp any eq 319 any
access-list 107 permit udp any eq 320 any
!
policy-map CIP-PTP-Traffic
 class CIP-Implicit_dscp_55
  set qos-group 1
 class CIP-Implicit_dscp_47
  set qos-group 1
 class CIP-Implicit_dscp_43
  set qos-group 1
 class CIP-Implicit_dscp_any
  set qos-group 2
 class CIP-Other
  set qos-group 2
 class 1588-PTP-Event
  set qos-group 0
 class 1588-PTP-General
  set qos-group 1
!
policy-map PTP-Event-Priority
 class qos-group-0
  priority level 1
 class qos-group-1
  bandwidth remaining percent 40
 class qos-group-2
  bandwidth remaining percent 40
 class class-default
  bandwidth remaining percent 20
!
```

```
class-map match-any 1588-PTP-General
 match access-group 107
class-map match-any 1588-PTP-Event
 match access-group 106
class-map match-any CIP-Other
 match access-group 105
class-map match-any CIP-Implicit_dscp_any
 match access-group 104
class-map match-any CIP-Implicit_dscp_43
 match access-group 103
class-map match-any CIP-Implicit_dscp_47
 match access-group 102
class-map match-any CIP-Implicit_dscp_55
 match access-group 101
!
class-map match-any qos-group-2
 match qos-group 2
class-map match-any qos-group-1
 match qos-group 1
class-map match-any qos-group-0
 match qos-group 0
!
```

Cisco IND Plug-and-Play

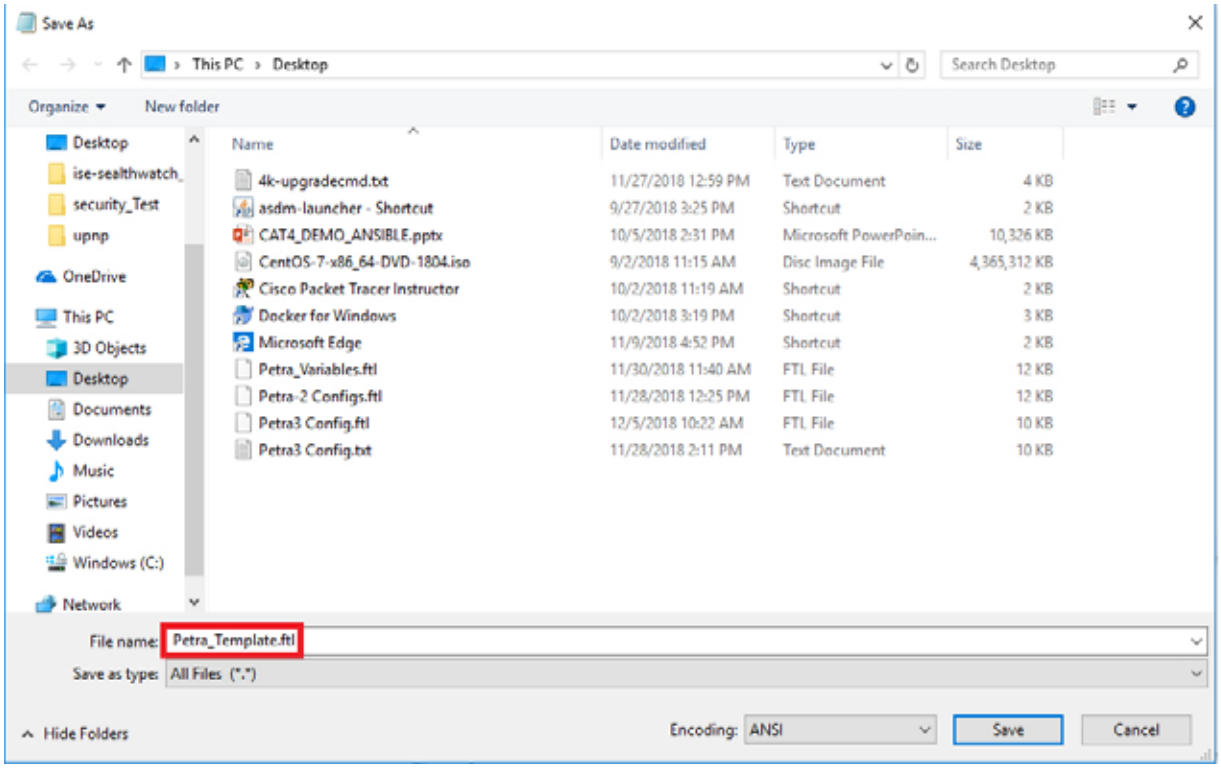
The Cisco IND plug-and-play feature provides the OT technician with a way to efficiently replace or add a new network device to their current network topology. The following section describes the steps to add a device to an existing ring using a configuration template in the IND plug-n-play feature.

Creating a Template

IND requires a template to be saved with a .ftl file extension (Apache FreeMarker™). The template is created using a copy of standard configuration on an existing switch. Values that may change, like host names, are replaced with input variables that are set before deploying the configuration to a new device. The template is saved with a .ftl extension by utilizing **File** -> **Save As..** and changing the .txt extension to .ftl.

Note: If you are copying a running configuration and modifying it as a template, be sure to remove any crypto self-signed certificate configurations. If you push a configuration with a certificate in the template, the self-signed certificate will be overwritten with the old one and will prevent the web UI from functioning.

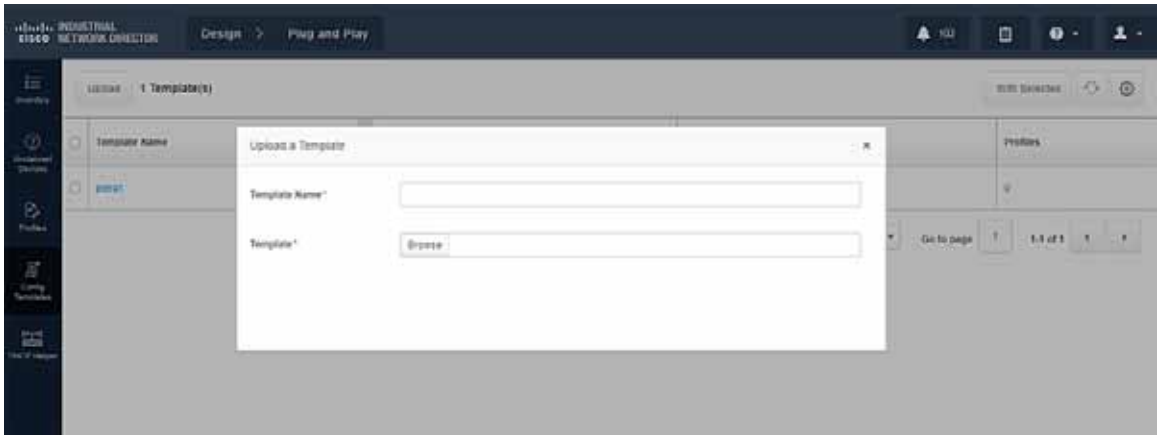
Figure 1 Replacing File Extension



Loading a Template

Go to **Design -> Plug and Play -> Config Templates -> Upload** and select the template previously created.

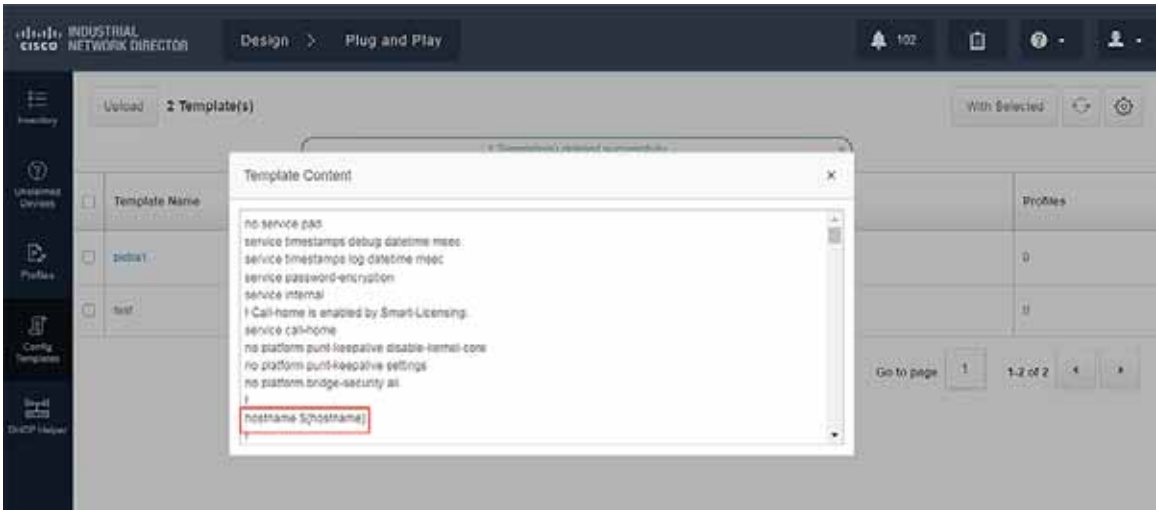
Figure 2 Loading Template



Template Validation

In the current template you will notice the ${hostname} variable. Using the dollar sign ($) and curly brackets ({}), you can define a variable in a template that will require the user to input the required value when pushing the configuration.

Figure 3 Template Validation



Configuring a Device for Plug-and-Play

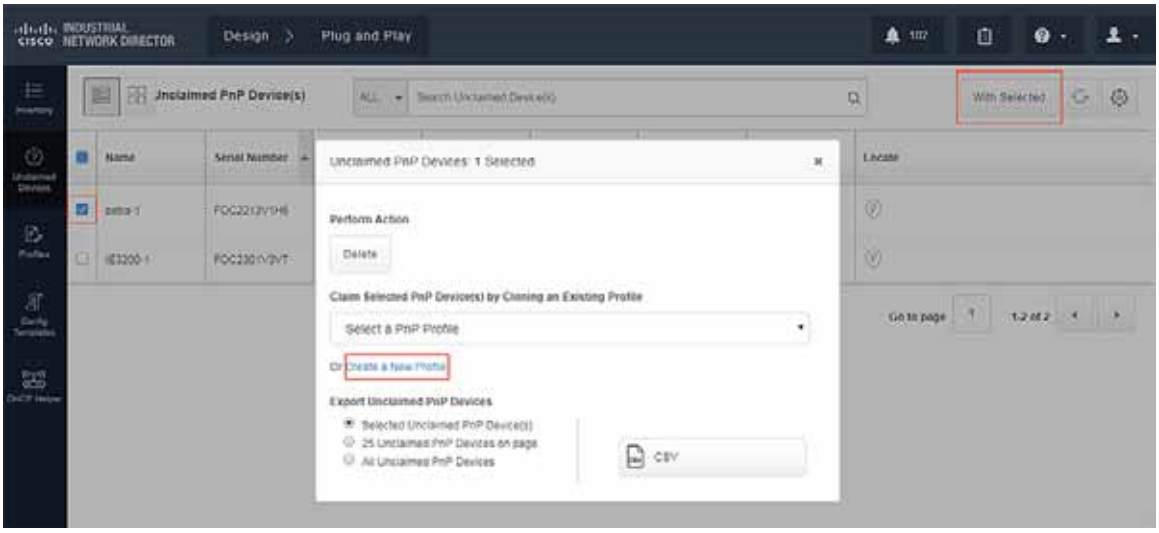
Out of the box, a switch will guide you through initial configuration, such as switch name, management, interface, and so on. Ensure the IP address of the device is reachable by IND. After initial configuration, configure the device to utilize plug-and-play with IND:

```
pmp profile profile-name
transport http ipv4 IND_IP_address port 8088
```

Pushing Configuration Template

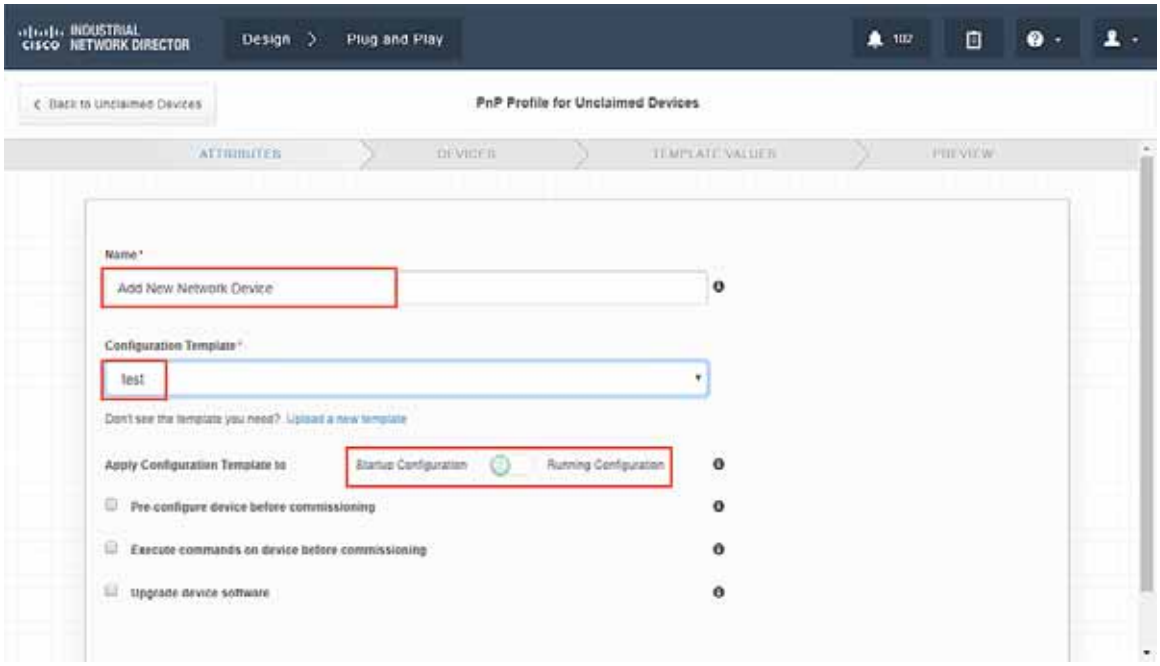
1. Once the device is configured, you should see the device under **Design -> Plug-and-Play -> Unclaimed Devices**. You should now be able to select the device to push a configuration template.

Figure 4 Pushing Template to New Device



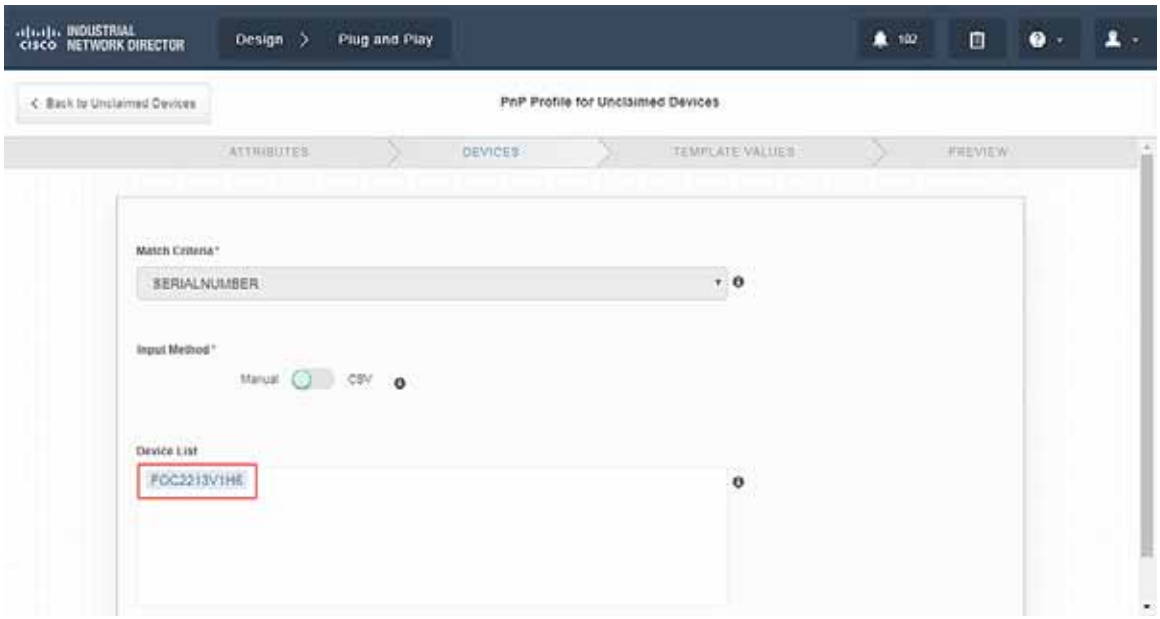
2. To push a configuration template, we must first create a new profile to define some attributes.

Figure 5 Create New Profile



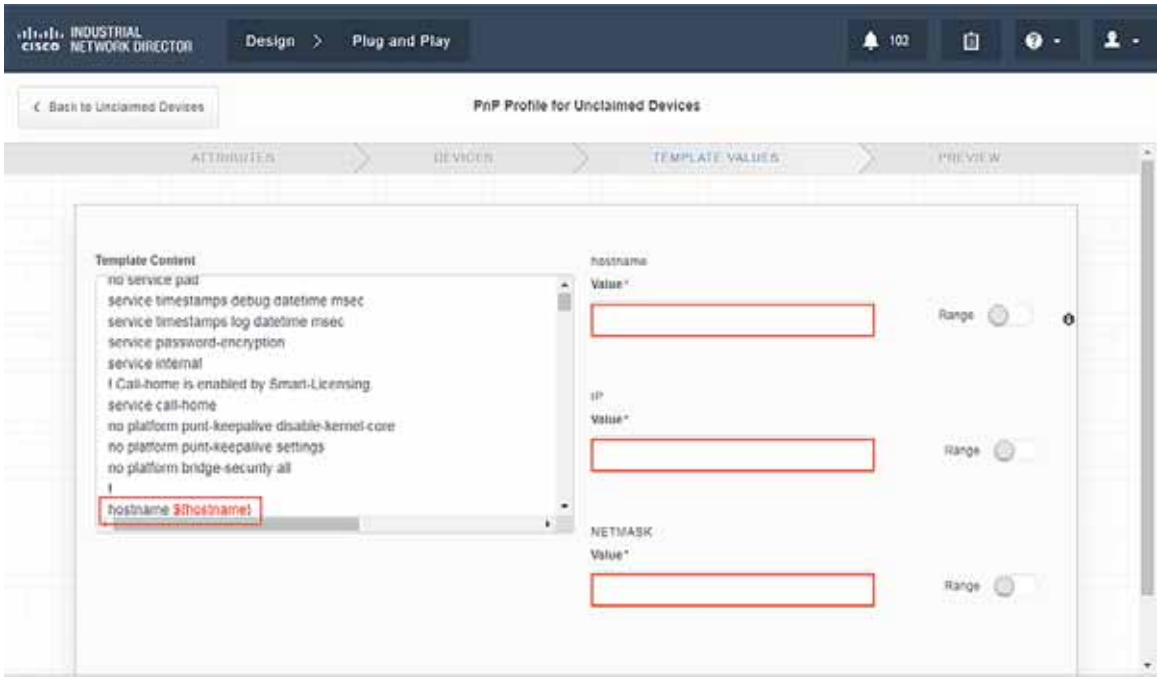
3. Devices that need to be configured are matched via serial number.

Figure 6 Device Matching



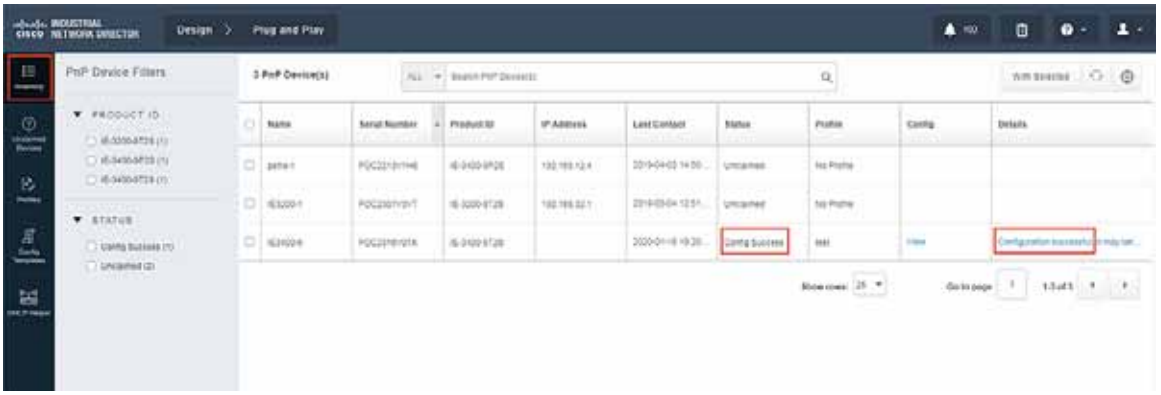
4. Enter the proper values in the variable fields.

Figure 7 Template Values



5. Validate that the configuration is correct and click **Claim**.
6. Verify that the new device has been configured correctly. The status should read **Config Success**.

Figure 8 Verifying Device Creation



Cisco Industrial Network Director Configuration

Cisco IND provides an easy-to-use interface designed especially for operations staff to be able to get a clear picture of their plant floor network and attached automation endpoints. For additional information, refer to the official product documentation available at:

- http://www.cisco.com/go/ind

- Network Management for Operational Technology in Connected Factory Architectures
  https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/IND/IND_Connected_Factory_CRD/IND_Connected_Factory_CRD.html

This section describes the validated configuration of IND, highlighting the following features:

- Creation of Discovery Profiles for IACS assets and networking devices.
- Creation of Device Access Profiles that will be used in discovering IACS assets and networking devices.
- Creation of Groups for IACS assets and networking devices based on the Cell/Area Zones.

Installation

The installation notes for IND can be found at:
https://www.cisco.com/c/en/us/td/docs/switches/ind/install/IND_1-4_install.html

Creating a Discovery Profile

The objective of creating a discovery profile is to define an IP address scope of different IACS assets and networking devices and scan those assets. If the IACS or networking device is reachable, then IND scans the device, discovers the attributes, and moves them to the IND inventory. Figure 9 shows how different asset discovery profiles are defined in IND.

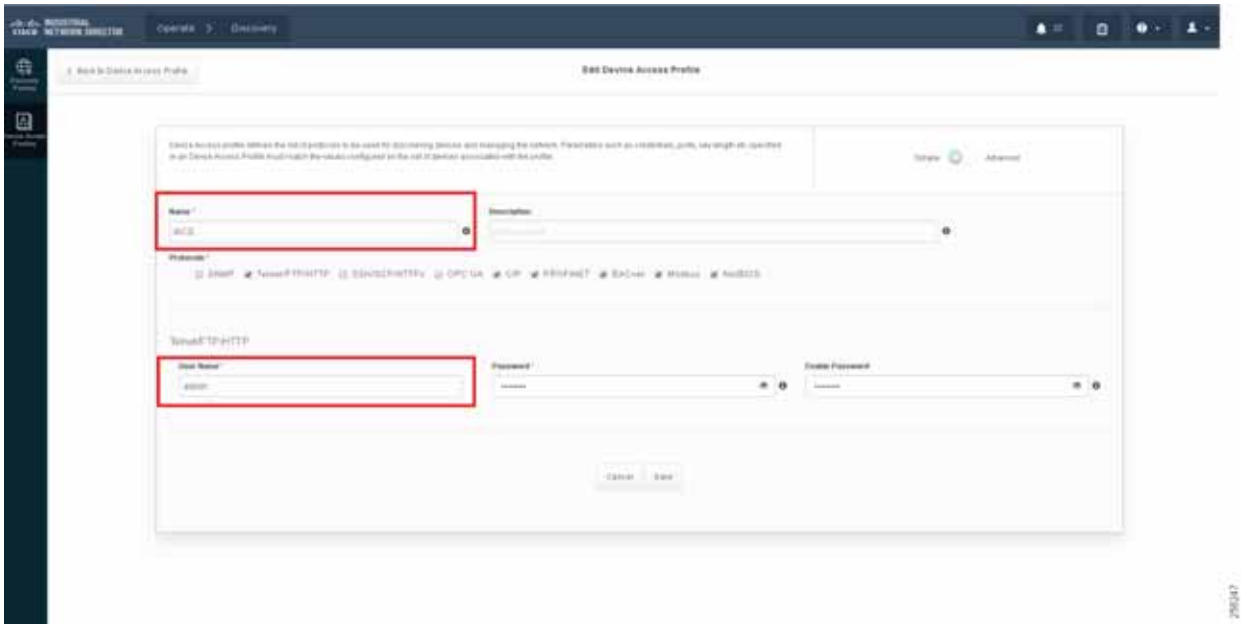
Figure 9 Creating the Asset Discovery Profile

As shown in the first row of Figure 9, the IACS profile is performing an IP scan for the IP address range 10.17.10.1-10.17.10.254. The Access_Profile used for this scan is IACS_PROFILE (explained in the next section) and all these devices are attached to a group called IACS_devices (also explained in the section below).

Configuring Access Profiles

The Access Profile is a template that has the common configuration parameters: username, password, and the SNMP community string information. When a group of devices use a different set of parameters, then a separate Access Profile can be defined. The Access Profile created in this section is tied to the Discovery Profile. Figure 10 shows the details of an Access Profile.

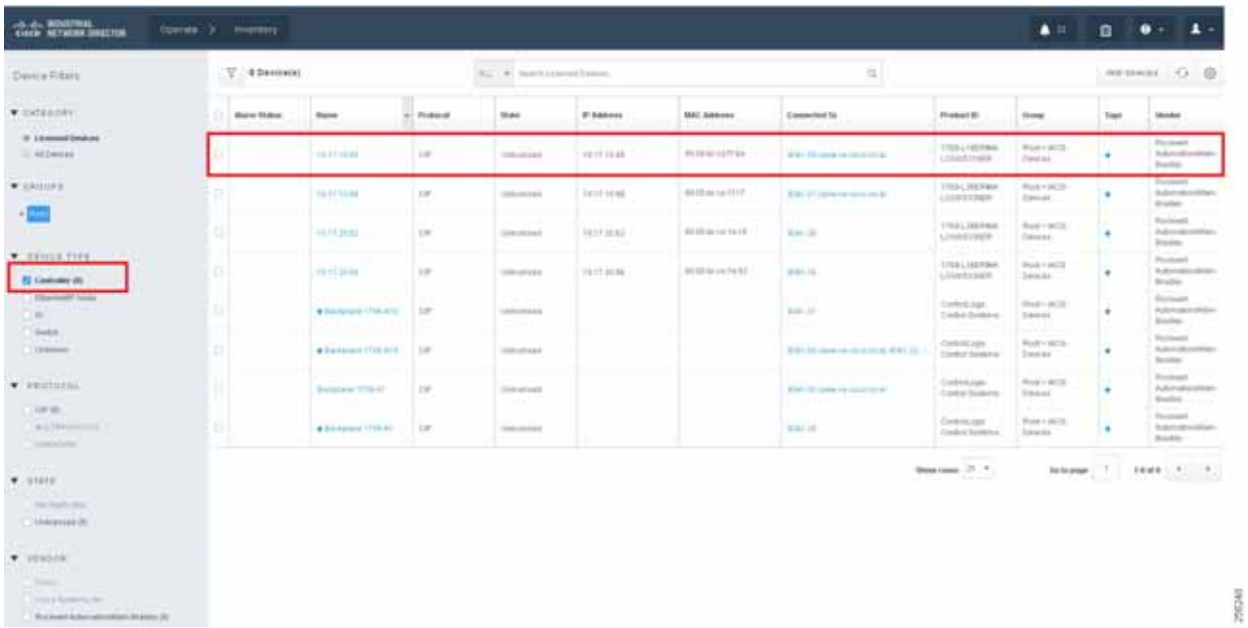
Figure 10 Configuring the Access Profile



Asset Inventory

IND maintains list of devices that it has discovered in the Inventory. For each Inventory item, details such as uplink device, IACS type (for example, Controller or I/O), the interface between the IACS device and the switch, the protocol used to communicate with the IACS asset, IP address of the IACS asset, Group, vendor information, and so on. There are filters available for OT control system engineers to search for devices based on different criteria. Figure 11 shows a list of controllers that support the CIP protocol. As shown in Figure 11, IND displays important information about the IACS asset.

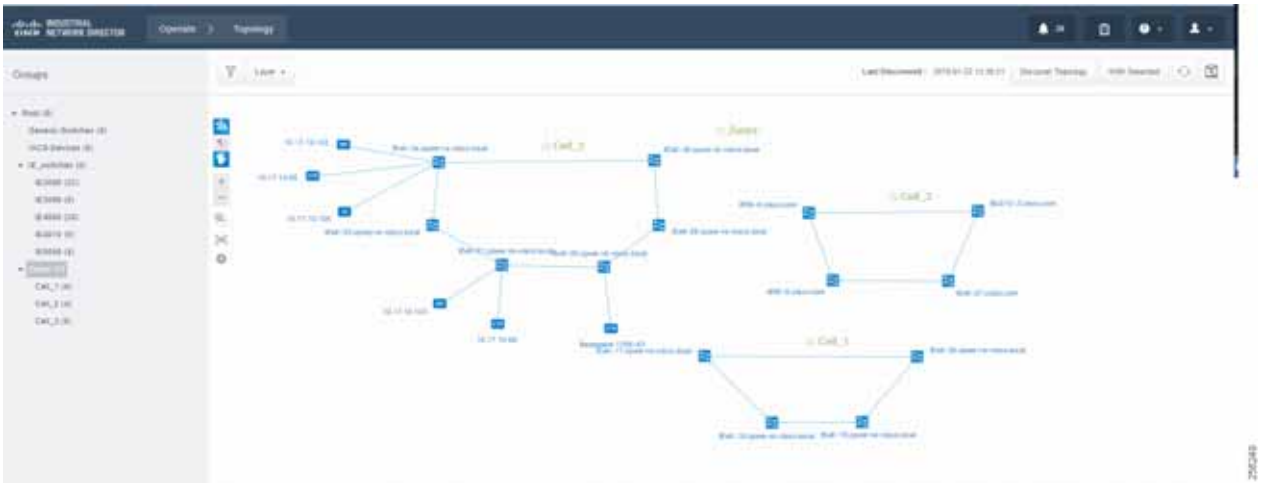
Figure 11 Asset Inventory of IND



Group Management

Managing devices in separate groups simplifies the management of devices. Figure 12 shows three groups that have been created based on the Cell/Area Zone topology.

Figure 12 Topology Diagram for IND



Licensing

IND comes up with a base license that allows an OT operator to create Discovery Profiles to scan assets as well as use plug-and-play to configure assets. However, certain features of IND for managing IES devices require an additional license purchase.

For more information on IND licensing, see:
https://www.cisco.com/c/dam/en/us/products/collateral/cloud-systems-management/industrial-network-director/datasheet-c78-737848.pdf

IND Configuration for Precision Time Protocol

IND for Precision Time Protocol (PTP) infrastructure discovery and management requires CIP and Simple Network Management Protocol (SNMP) features and begins with IND release 1.7. It includes the following steps:

- Industrial network devices discovery
- Industrial network devices inventory and licensing
- Industrial network devices PTP topology and PTP attributes validation

System Requirements

Table 1 System Requirements

Desktop Requirements	Minimum Requirement
Windows Operating System (OS)	Windows 7 Enterprise or Professional with Service Pack 2 or Windows 10 Windows Server Support: Windows 2012 R2 Server Windows 2016 Server (64-bit version) **Note:** When using Windows 2016 Server (64-bit version), you may not be able to select the Uninstall option from the Windows Start program window. If this occurs, log out of Windows 2016 and then log in again. If you do not see the Uninstall option in the Windows menu, then restart the PC.
Browser	Chrome: Version 50.0.2661.75, 53.0.2785.116 Firefox: 55.0.3, 57.0.4,63.0.3 or above
CPU	Quad-Core 1.8 GHz
RAM	8 GB
Storage	50 GB

The IND software package requires:

- No other FTP server is running and listening on port 21.
- No other instance of PostgreSQL is installed on port 5432 or any other port on the system.
- The host name of the Windows machine must start with a letter of the alphabet (A-Z or a-z).
  - You may use special characters within your password such as digits (0-9), minus sign (-), and period (.) as well as alpha characters.
- The following ports are open for both inbound traffic on the firewall:

  TCP ports:

  - 21—FTP active port for ODM file transfer in regular mode
  - 8088—HTTP for PnP
  - 8443— HTTPS for Web UI and PnP
  - 50000-50050—FTP passive ports for ODM file transfer in regular mode

  UDP port:

  - 30162—SNMP traps
- The following ports are open for outbound traffic on the firewall:

  TCP ports

  - 443—HTTPS for WSMA/JSON-RPC in secure mode
  - 80—HTTP for WSMA/JSON-RPC in regular mode
  - 22—SSH/SCP in secure mode

- 23—Telnet in regular mode
- 44818—CIP
- 102—PROFINET
- 502—ModBus
- 4840—OPC-UA
- 139—NetBios TCP/IP
- 1812—RADIUS

UDP ports:

- 161—SNMP
- 67—DHCP server if the IND PnP DHCP helper is being used
- 2222—CIP
- 34964—PROFINET
- 4840—OPC-UA

- The following ports are open for both inbound and outbound traffic on the firewall:

  TCP ports:

  - 8910—HTTPS for pxGrid
  - 47808—BacNet

Note:

- The above listed ports are default ports. If any of the above ports are customized as part of the installation or in an access profile, then the corresponding ports should be open in the firewall.
- The network device local user needs to have privilege level of 15.

IND Industrial Network Devices Discovery

IND for PTP discovery requires the following features to be enabled in industrial network devices:

- CISCO-PTP-MIB for SNMP supported devices
- CIP object 43 for CIP supported devices

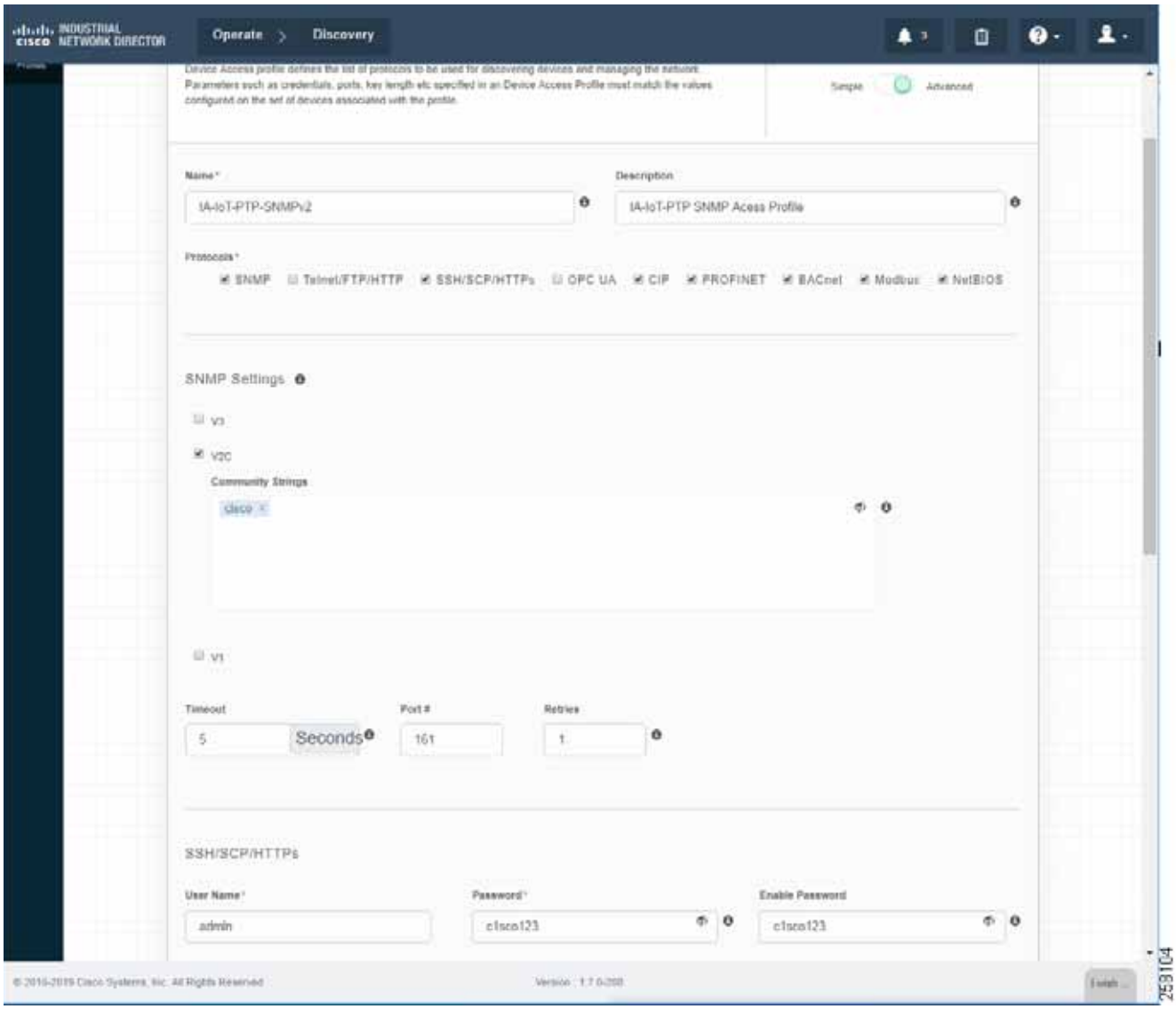
In order for Industrial network devices to be discoverable by IND, the following SNMP and CIP related configuration needs to be manually enabled:

```
IE5K-1#show run int vla 18
!
interface Vlan18
 cip enable
end
!
IE5K-1#show run | inc snmp
!
snmp-server group IA-IoT-PTP v2c
snmp-server community cisco RW
!
```

Creating Device Access Profiles

Create a Device Access Profile and provide the corresponding SNMP community string and version setting, Select the **Advanced** option to provide SSH or Telnet related credentials as shown in Figure 13.

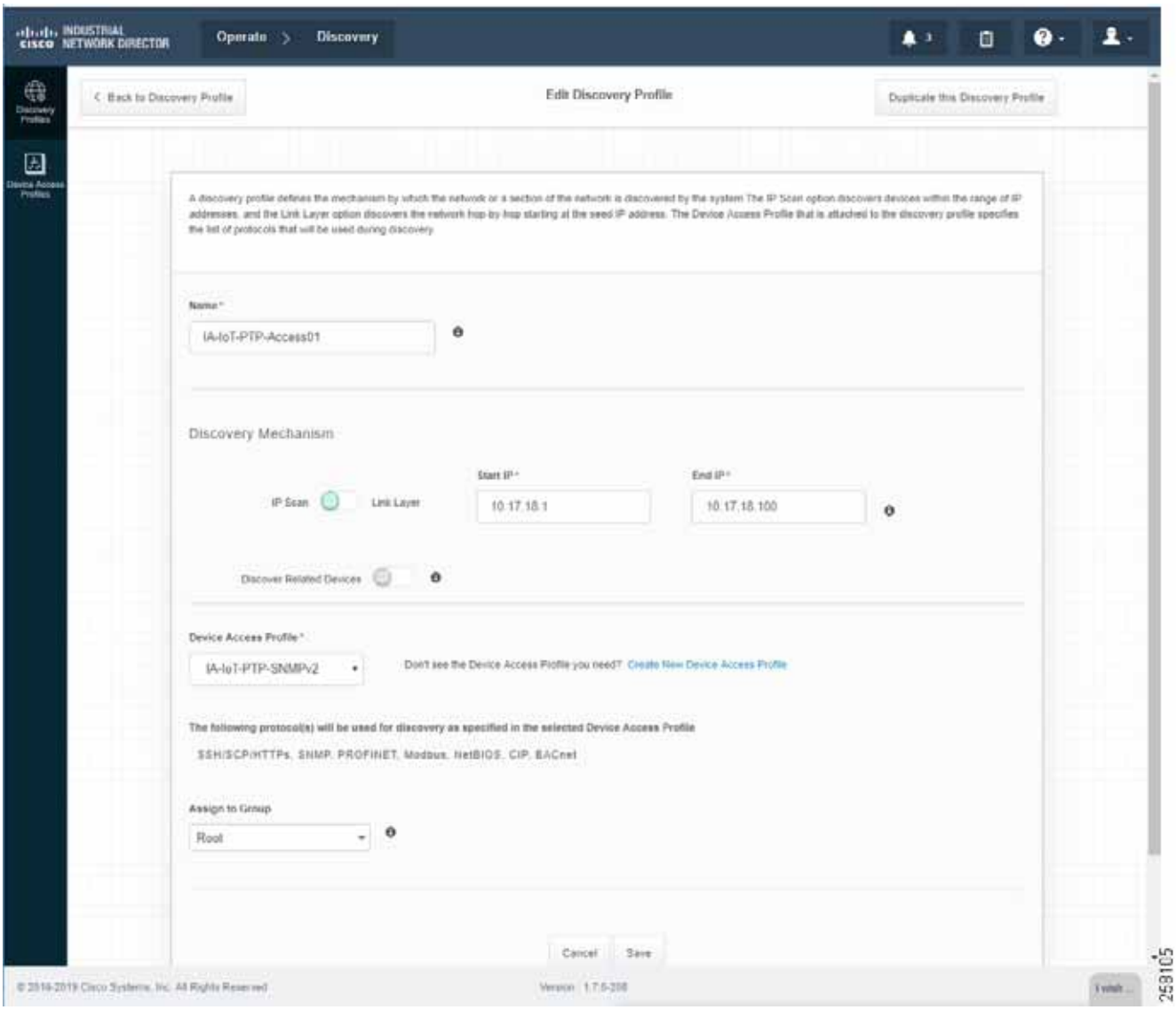
Figure 13 Creating Device Access Profile



Creating Device Inventory with IP Scan

Based on the network infrastructure and IP address mapping, create an IP Scan Discovery Profile as shown in Figure 14.

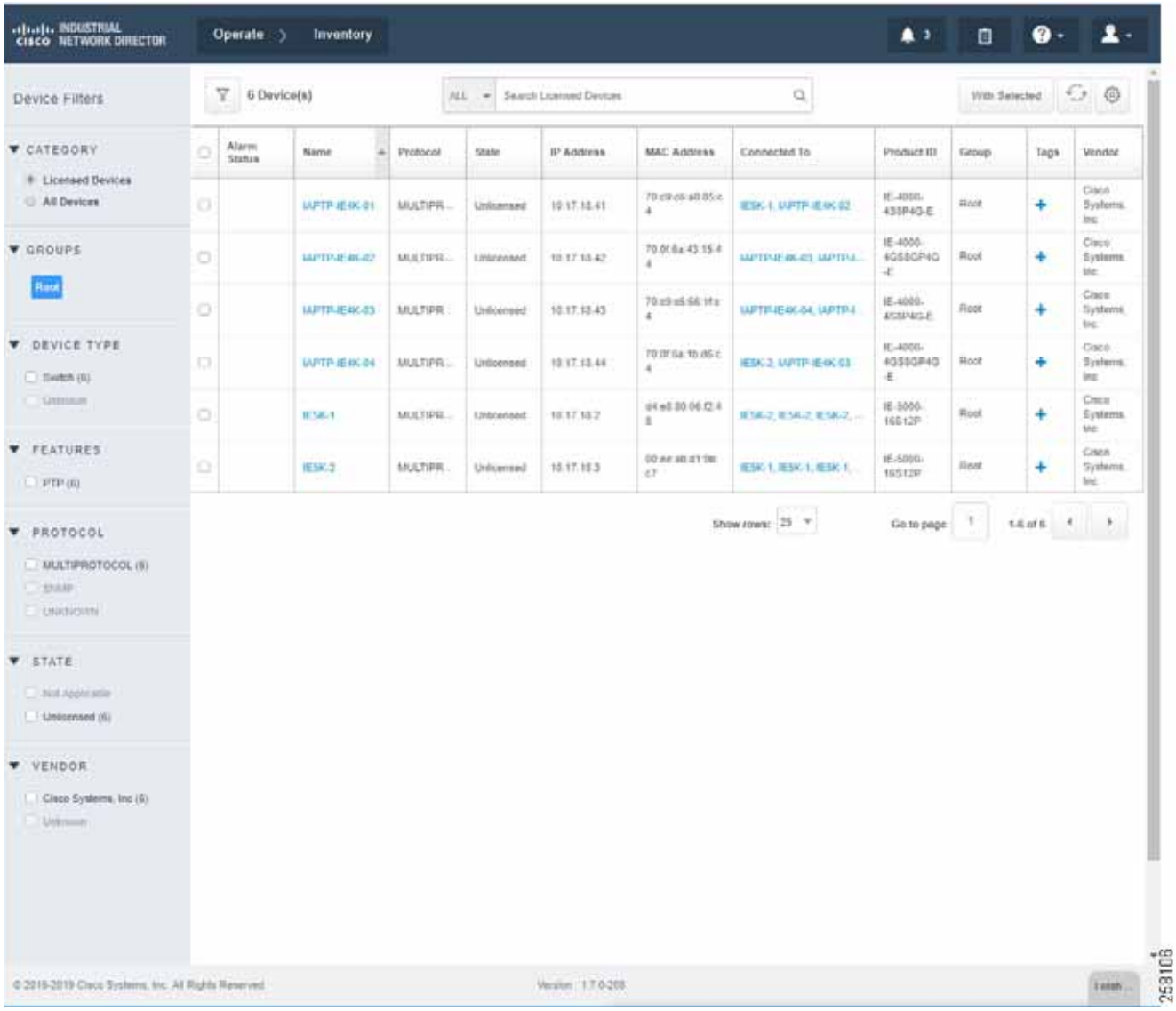
Figure 14 Creating Device Inventory with IP Scan



Device Discovery is based on SNMP MIB and related CIP features being enabled inside network devices. IND IP Scan will send an SNMP probe as specified in the Device Discovery Profiles IP address range above and populate Inventory tables and constructs device connectivity in the background. Figure 15 shows the populated Inventory table; each inventory device reflects its detailed device related information.

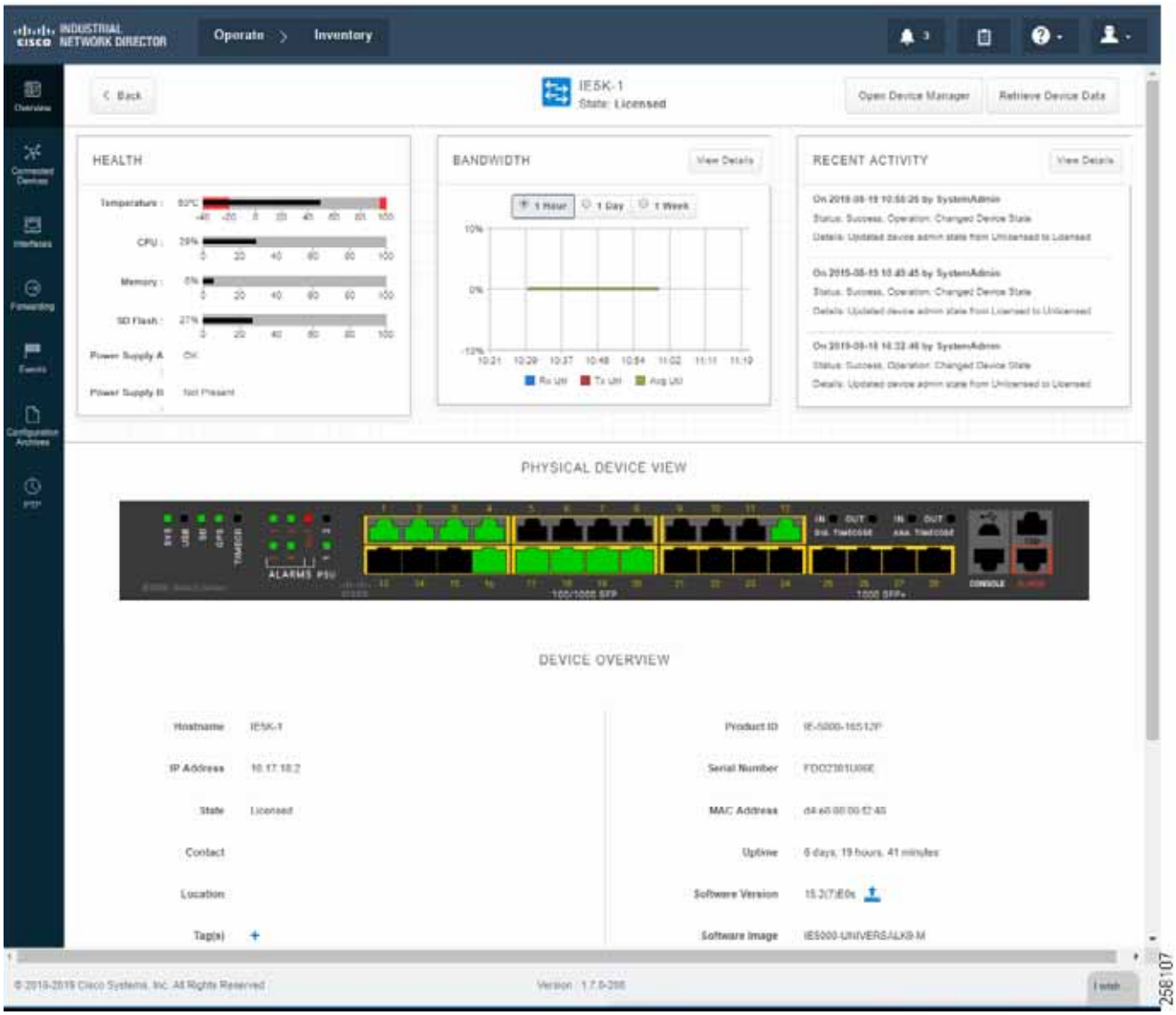
Industrial Network Devices are started inside IND in an “Unlicensed” state as shown in Figure 17.

Figure 15 IND in Unlicensed State



Industrial Network Devices have to be toggled into a “Licensed” state for management PTP related features as shown in Figure 16.

Figure 16 IND Inventory Device Detailed Status



During the license state change, a boostrap configuration is pushed into each of the network devices to enforce license subscription management. The following is a boostrap sample configuration:

```
Bootstrap Configuration
The system pushes the following configuration when you move the device to the Licensed state in the
system:
# Secure-mode only
# Only if user selected self-signed certificate for device certificate in access profile
# If the device has a self-signed certificate with RSA key pair length < certificate key length given
in access profile (or) if the device does not have a self-signed certificate in nvram
crypto key generate rsa label IND_HTTPS_CERT_KEYPAIR modulus {certificate-key-length}
crypto pki trustpoint IND_HTTPS_CERT_KEYPAIR
enrollment selfsigned
subject-name OUT="IOT"
rsakeypair IND_HTTPS_CERT_KEYPAIR
hash sha256
crypto pki enroll IND_HTTPS_CERT_KEYPAIR
# Enable SCP server
# Used for transferring ODM file from the system to device
```

```
# For insecure mode the system uses FTP to transfer ODM file
ip scp server enable

# If AAA is not enabled on the device
ip http authentication local
#Secure mode only
ip http secure-server
ip http secure-port {secure-mode-access-port}
#Insecure mode only
ip http server
ip http port {regular-mode-access-port}

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

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

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

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

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

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


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

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


# Turn on notifies for selected facility alarms
alarm facility temperature primary notifies
alarm facility temperature secondary notifies
# Following not application for CGS2K, IE3010
alarm facility power-supply notifies
no alarm facility power-supply disable
Bootstrap Configuration for IE 1000 Switches
# Traps for IE 1000
snmp.config.trap_source.add coldStart
snmp.config.trap_source.add warmStart
snmp.config.trap_source.add linkDown
snmp.config.trap_source.add linkUp
snmp.config.trap_source.add topologyChange
snmp.config.trap_source.add authenticationFailure
snmp.config.trap_source.add entConfigChange
snmp.config.trap_source.add fallingAlarm
snmp.config.trap_source.add risingAlarm
snmp.config.trap_source.add newRoot

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

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

Figure 17 IND License Apply into Industrial Devices

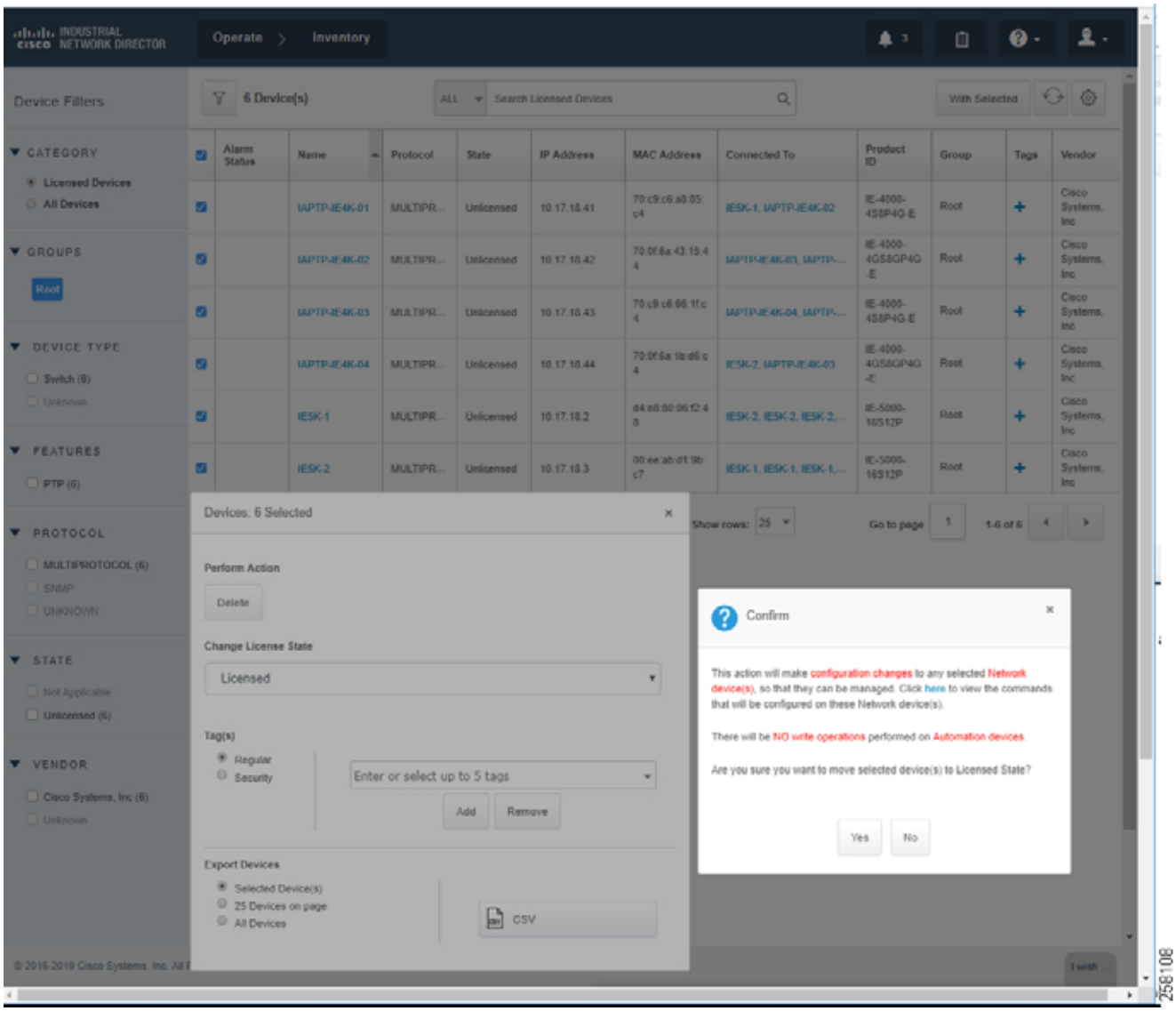
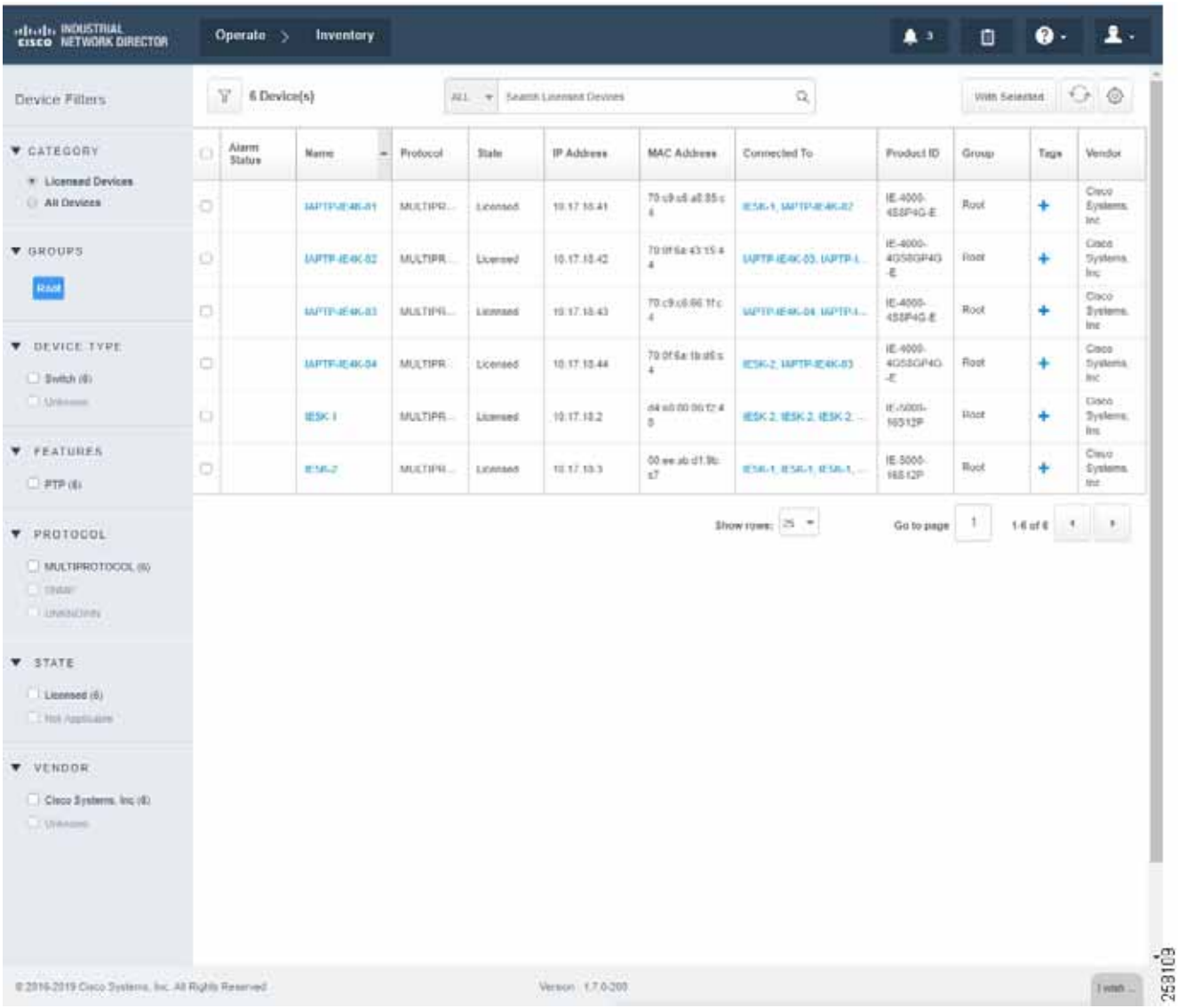


Figure 18 IND Inventory Devices Licensed State



Creating PTP Topology and Display PTP Attributes

For licensed industrial network devices, the IND topology will enable the PTP layer, which displays the PTP-related topology and each PTP device's attributes as shown in Figure 19, Figure 20, Figure 21, and Figure 22.

Figure 19 Topology and Device Attributes–PTP Hierarchy

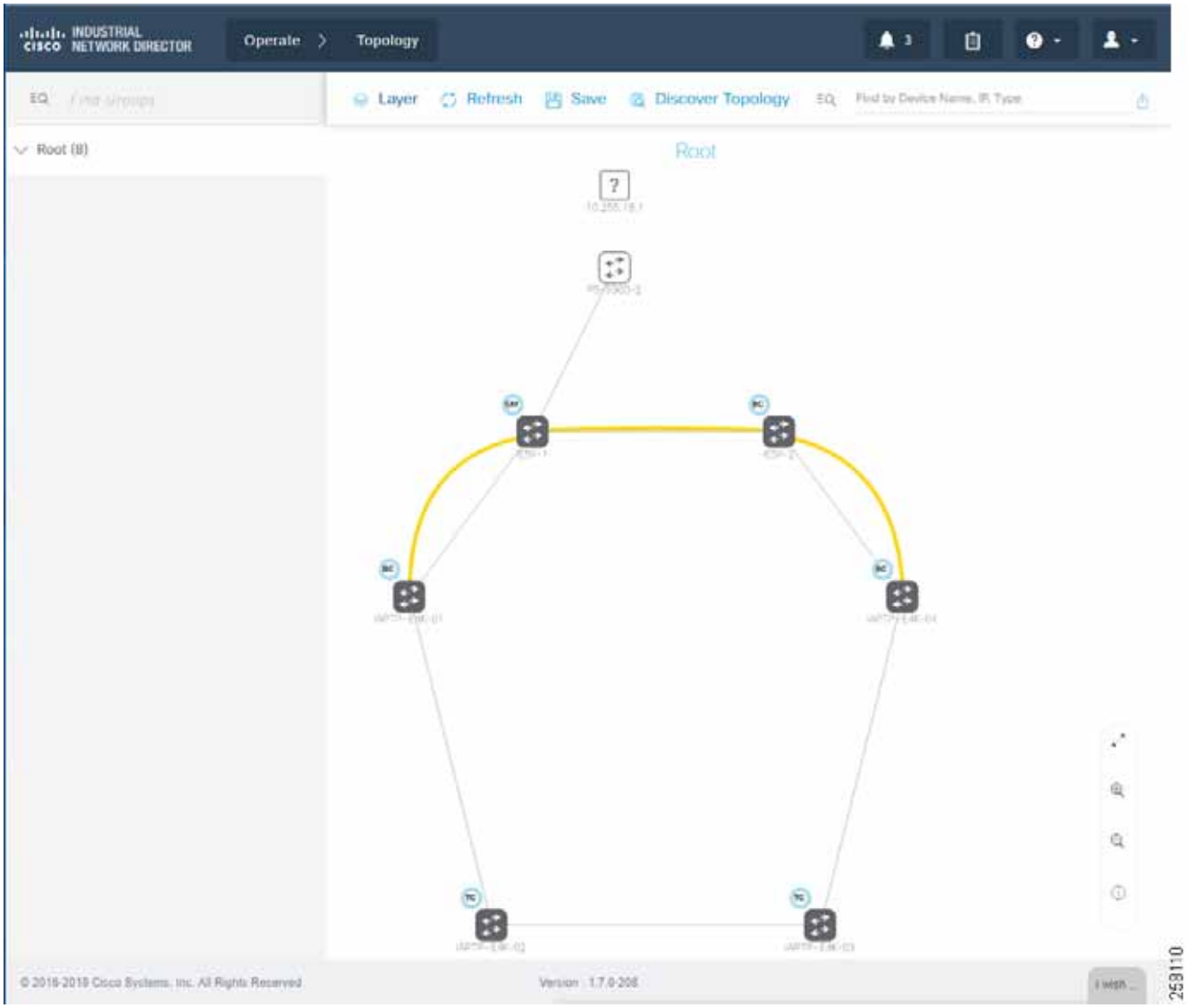


Figure 20 Topology and Device Attributes–PTP GrandMaster Device

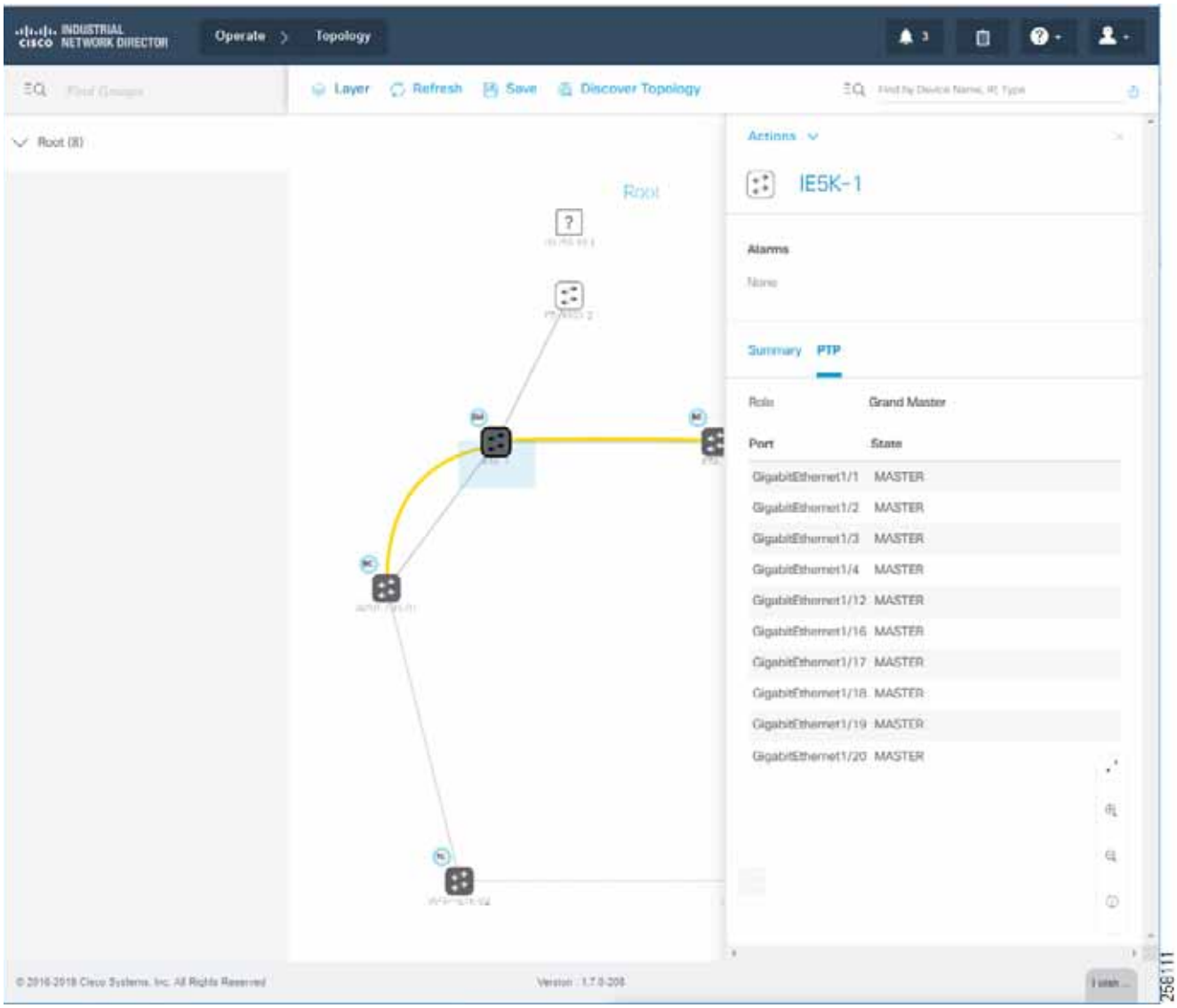


Figure 21 Topology and Device Attributes–PTP Boundary Clock Device

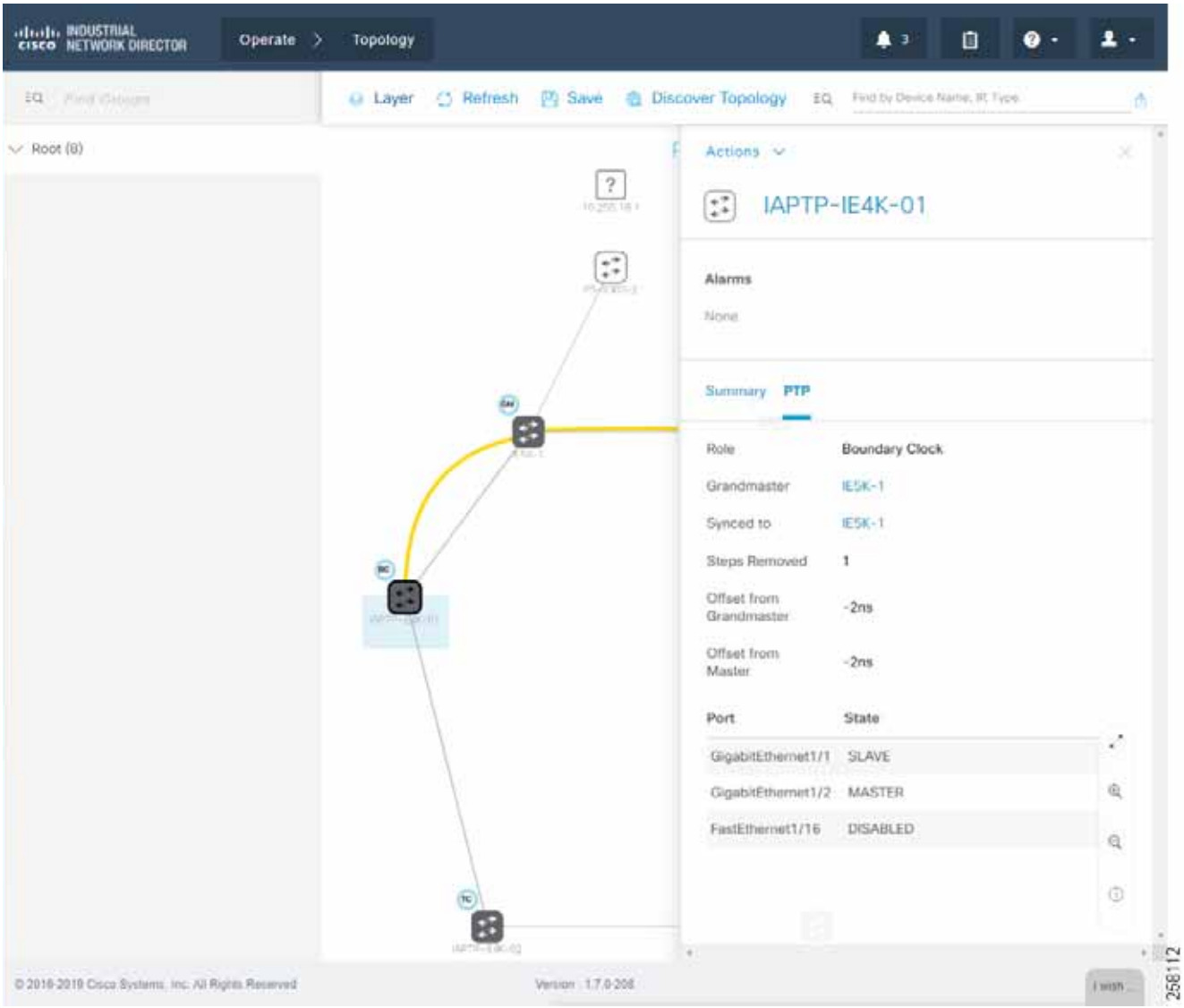
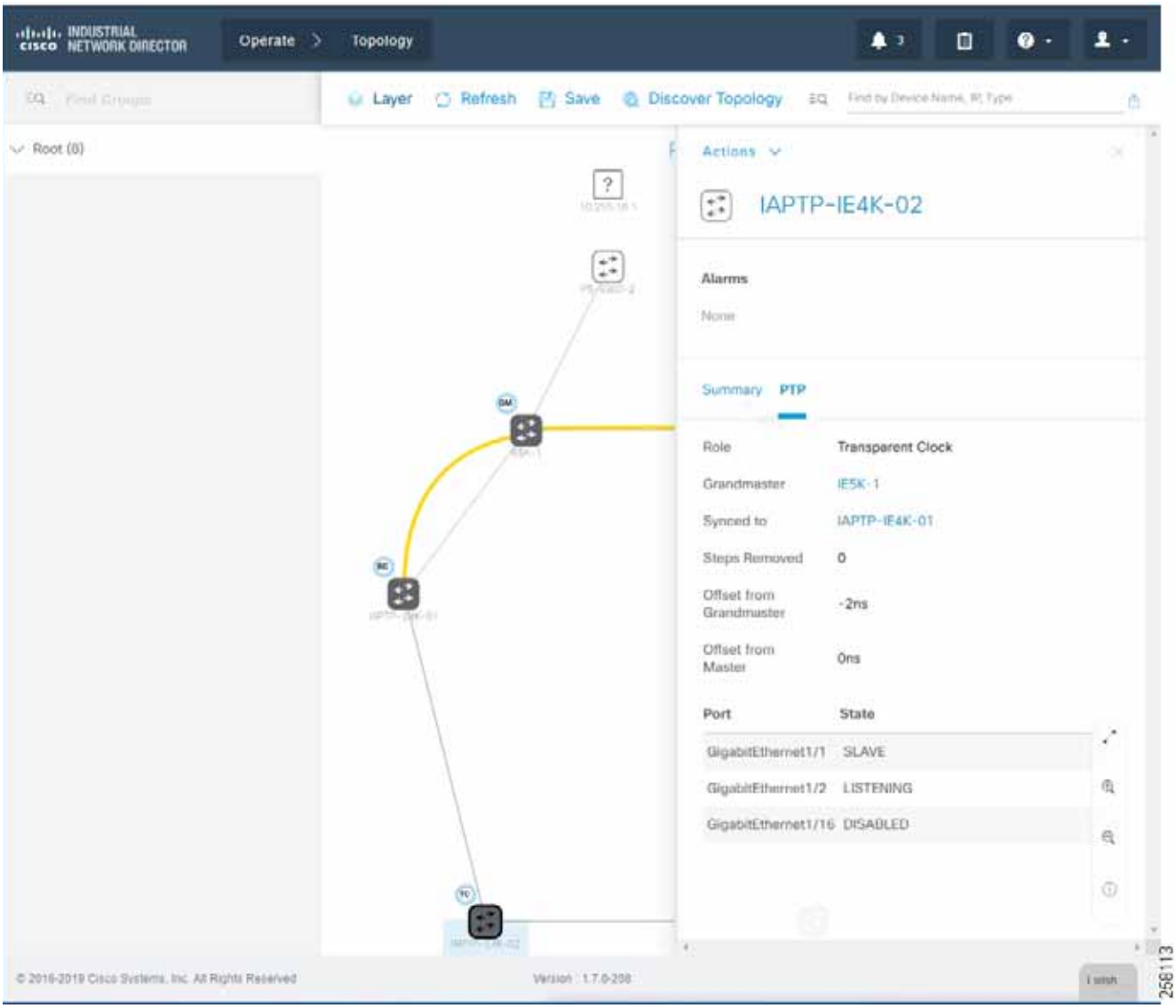


Figure 22 Topology and Device Attributes–PTP Transparent Device



Cisco ISE Configuration

This section gives details on how to configure Cisco ISE for the following components:

- Distributed deployment
- Enabling profiling and configuring different profiling policies
- TrustSec configuration

Distributed Deployment

The distributed deployment of ISE was validated for this CVD. Figure 23 shows how multiple ISE nodes are configured with various personas to achieve the distributed model.

Figure 23 Devices Present in Distributed ISE Deployment

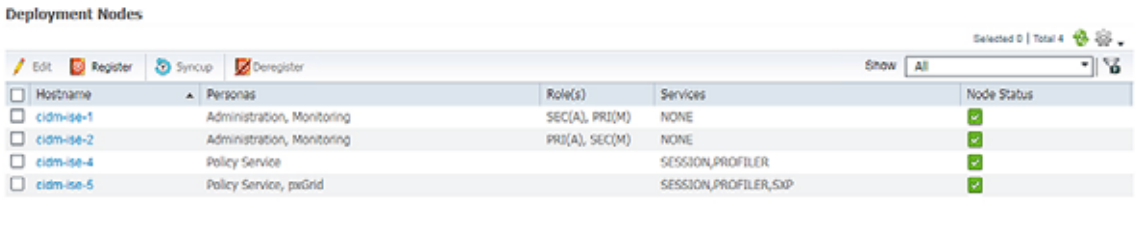


Table 2 describes the role for each of the ISE instances.

Table 2 ISE Instance Roles

Device Name	Role
cidm-ise-2	Primary Administration Node, Secondary Monitoring Node
cidm-ise-1	Secondary Administration Node, Primary Monitoring Node
cidm-ise-4	Policy Service Node
cidm-ise-5	Policy Service Node with pxGrid

As shown in Table 2, cidm-ise-2 is the PAN node for this design, and all the administration tasks such as configuration of network devices, authentication policies, authorization policies, certificate management, checking logs, and all other tasks must be done on this PAN. The PSNs are used for RADIUS and Cisco TrustSec (CTS) communication with the network access devices. In this deployment, since the PAN (cidm-ise-2) is not configured with the Policy Service Node persona, the network access devices must not point to the PAN.

Profiling Policies in Cisco ISE

This section shows how to create different profiling policies based on Table 3. The profiling policies shown here are meant as an example and should not be considered a method for the actual deployment.

Industrial Network Access Scheme

ISE profiling uses specific attributes to categorize devices, subsequently enabling authentication and authorization policies based on profile policy criteria. Table 3 gives an example on different roles for IACS assets in a plant-wide architecture. For example, an Engineering Workstation needs access to all the devices in the plant-wide architecture. Similarly, a device classified as Level_0_IO only has access to devices that are located in the immediate Cell/Area Zone. Based on the access scheme in Table 3, we can create profile, authentication, and authorization TrustSec policies to be manifested in a plant-wide network.

Table 3 Industrial Network Access Scheme

Device	Location in Plant-wide Network	Access Level
Engineering Workstation (EWS)	Level 3 site operations	Must have access to all the devices in the plant-wide architecture
Controller Interlocking (Level_3)	Cell/Area Zone	All the inter-locking PACs must have access to another inter-locking PAC
Level_2_HMI	Cell/Area Zone	LEVEL_2_HMI must have access to all the devices in Level_0 and Level_1
Level_1_Controller	Cell/Area Zone	Access restricted to a particular Cell/Area Zone
Level_0_IO	Cell/Area Zone	Access restricted to a particular Cell/Area Zone

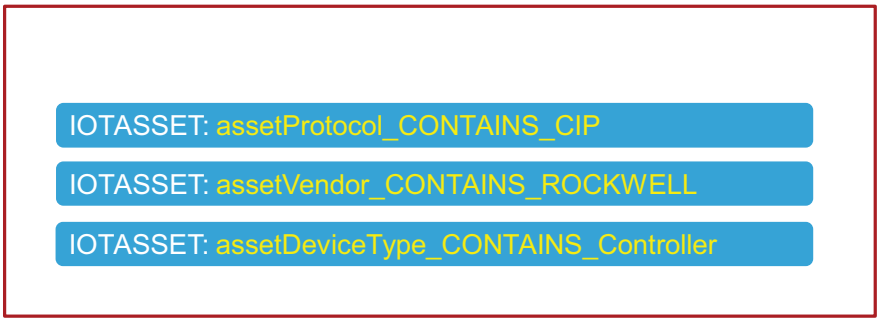
Table 3 Industrial Network Access Scheme (continued)

Device	Location in Plant-wide Network	Access Level
Level_0_Robot	Cell/Area Zone	Access restricted to a particular Cell/Area Zone
Level_0_Drive	Cell/Area Zone	Access restricted to a particular Cell/Area Zone
Level_0_Generic	Cell/Area Zone	Access restricted to a particular Cell/Area Zone
LOCAL_PARTNER	Cell/Area Zone	Access restricted to a particular Cell/Area Zone
REMOTE_ACCESS	Cell/Area Zone	Access to a remote desktop server
REMOTE_DESKTOP	Level 3 site operations	Access to a device with SGT value = REMOTE_ACCESS
Production user (PROD_USER)	Level 3 site operations	Access to all devices in the plant-wide architecture
Operator Workstation (OWS)	Level 3 site operations	Access to all devices in the plant-wide architecture

Level_1_controller Policy

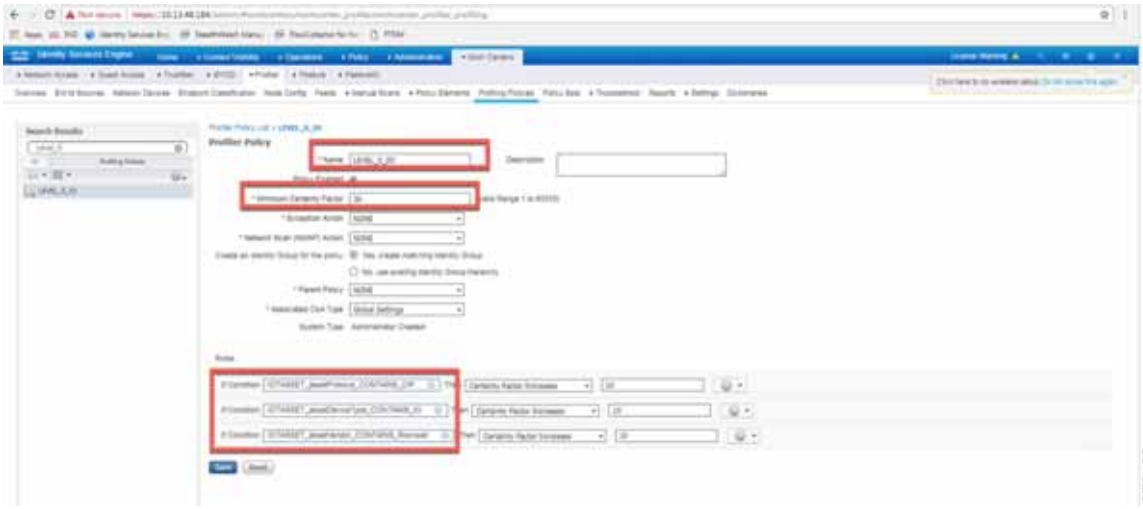
This policy is used to profile an IACS asset which is a controller. The key attributes used to profile this device are shown in Figure 24. As shown in Figure 24, the IOTASSET dictionary is used to match different conditions like protocol, assetVendor, and assetDeviceType. The values for the attributes assetVendor and assetDeviceType are obtained by ISE via the pxGrid integration with Cisco Cyber Vision. When a new IACS asset is discovered by Cisco Cyber Vision, it provides the details of the asset to Cisco ISE and this information is used to fill in the attribute values of the IOTASSET dictionary.

Figure 24 Attributes Used to Profile a Controller



When a match is found for each condition, the certainty of the device matching the profile increases. For example, in Figure 24, if each condition match gives a certainty factor of 10, then if all three conditions match the certainty factor becomes 30. The profiling policy can be tailored to be as strict as necessary; for example, only allowing a profile match if reached a certainty factor of 30, or alternatively profiling by matching at least one condition. In this CVD, the stringent choice was made when classifying a controller. Figure 25 shows the Level_1_controller policy defined in Cisco ISE.

Figure 25 Level_1_controller Policy in Cisco ISE



Level_0_IO Policy

The Level_0_IO policy is used to profile I/O assets, which usually only require local Cell/Area Zone communication. Figure 26 shows the profile conditions for Level_0_IO and Figure 27 shows the profiling policy used to profile I/O IACS assets.

Figure 26 Level_0_IO Profile

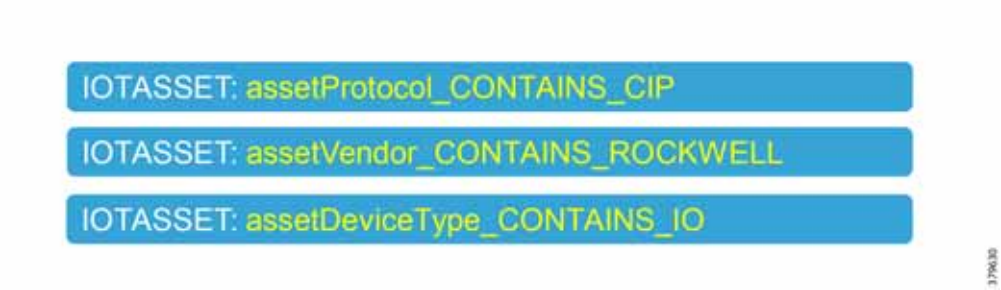
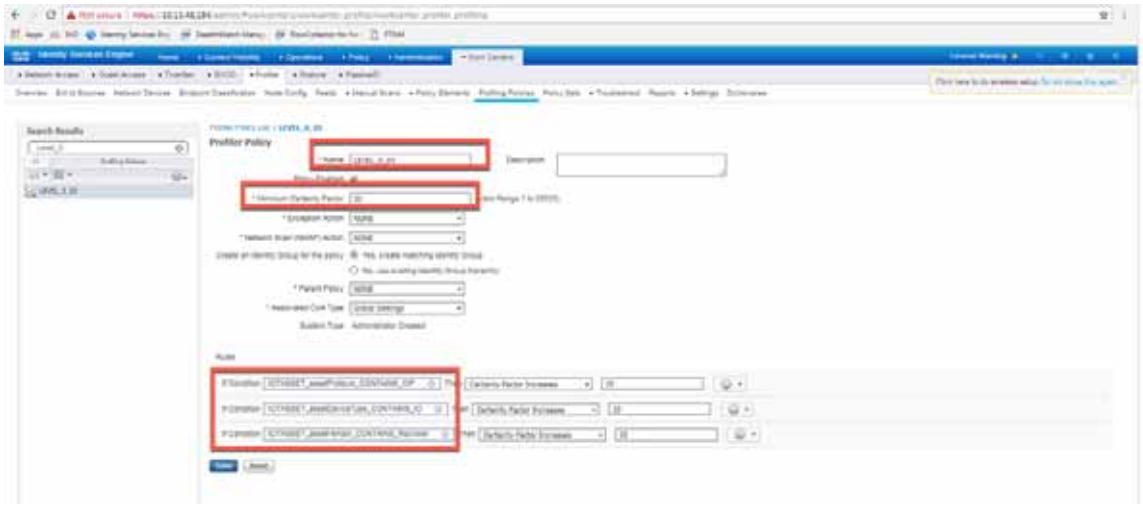


Figure 27 Level_0_IO_policy



Custom Attributes

Cisco ISE uses attributes defined in a dictionary to restrict access to IACS assets and other devices. In Figure 25 and Figure 27, IOTASSET dictionary was used to match attributes that were meant to match IACS assets. In addition, Cisco ISE allows a user to create custom attributes. A combination of pre-defined attributes provided by Cisco ISE along with user attributes allows an IT security architect to create more granular policies. In this CVD, the custom attribute assetGroup was used to create more granular policies. Cisco Cyber Vision provides the value for this attribute, which is then used in conjunction with default ISE attributes. Figure 28 shows how to define custom attributes in the Cisco ISE web UI under **Administration -> System -> Settings -> Profiling**.

Figure 28 Enabling Custom Attributes in Cisco ISE

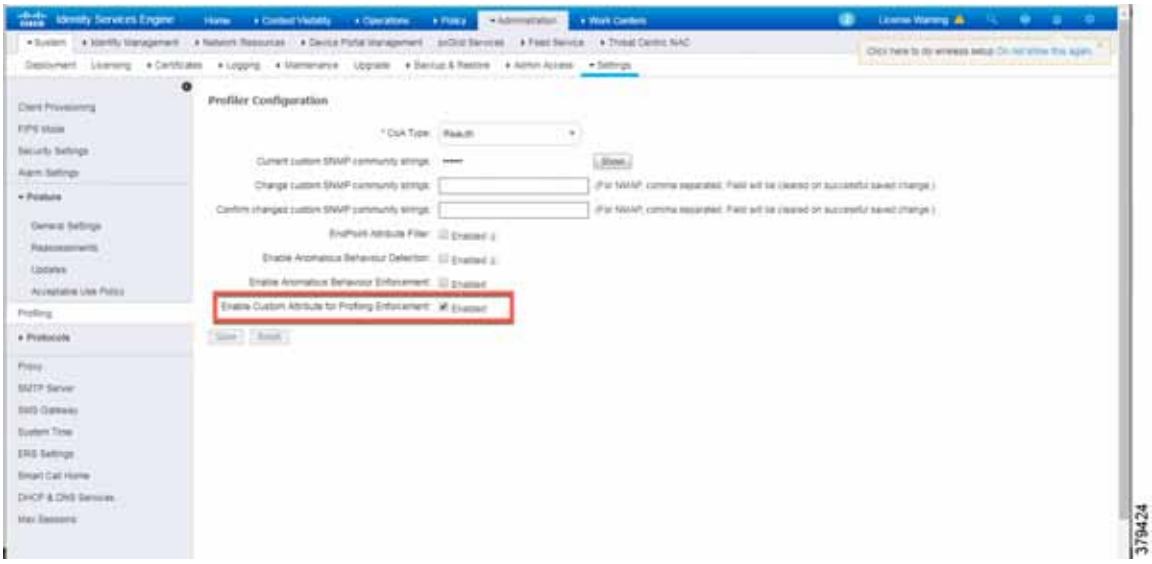
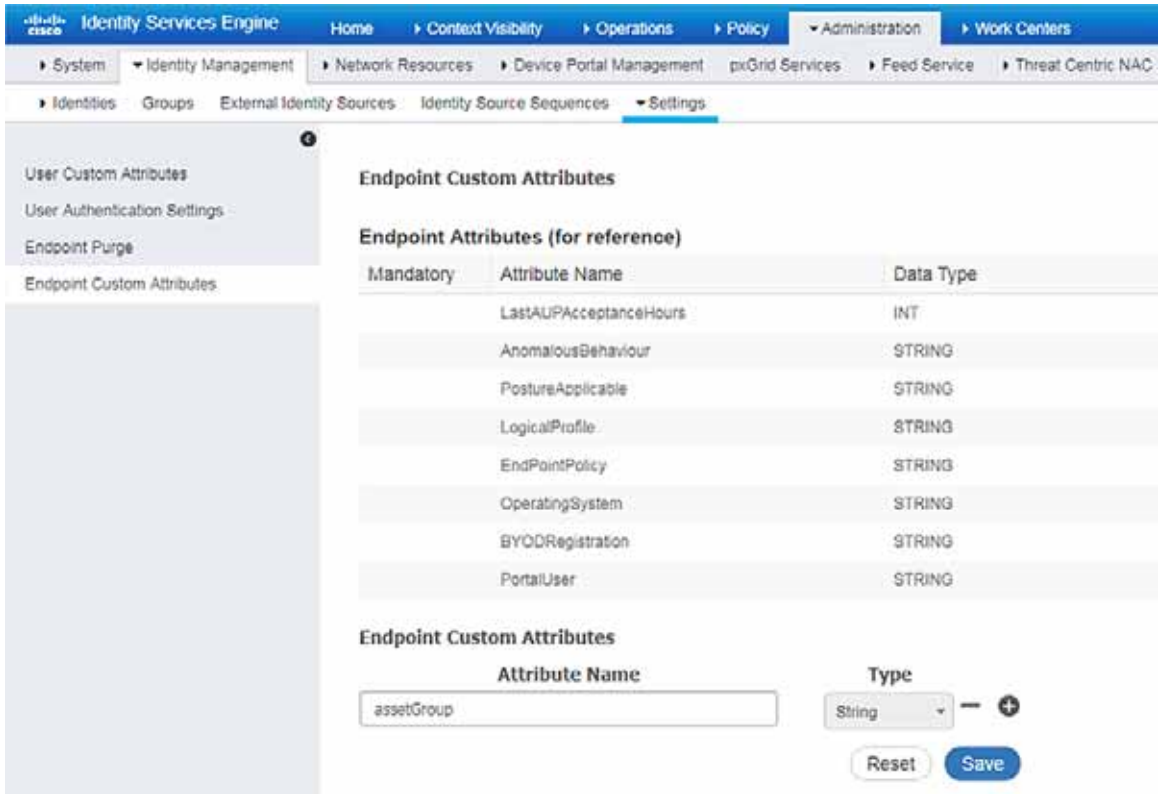


Figure 29 shows how to define the custom attributes by going to **Administration -> Identity Management -> Settings -> Endpoint Custom Attributes**.

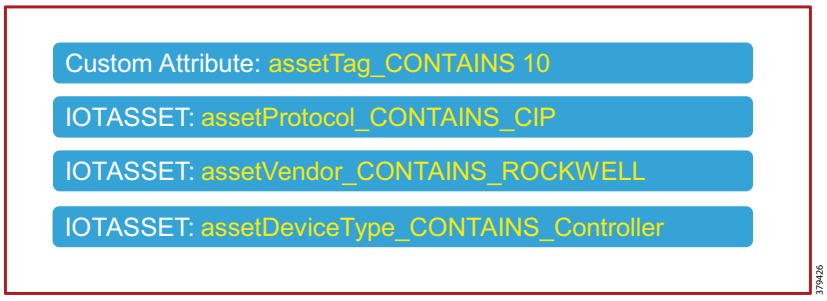
Figure 29 Custom Attribute Examples



Level_3 Policy

The Level_3 policy is used to profile IACS assets that need to access IACS assets across the Cell/Area Zones. For example, a Level_1_Controller in a Cell/Area Zone may need to access another Level_1_Controller in another Cell/Area Zone. This access may not be needed for all the Level_1_Controllers, but only for a few of them. Cisco ISE profiles a device as a Level_1_Controller based on the device attributes defined in the IOTASSET dictionary. In addition, a custom attribute is used to differentiate this device as Level_3. Figure 30 shows the general idea of classifying the device as Level_3.

Figure 30 Level_3_Policy



The assetGroup attribute is a custom attribute that was used in addition to the device attributes such as assetProtocol, assetVendor, and assetDeviceType. The minimum certainty factor now increases to 40 because four attributes are used to match an IACS asset as Level_3 and each attribute has certainty factor of 10.

Remote_Access

This profiling access policy is used to classify IACS assets that are made temporarily accessible by a remote user for support and maintenance. For example, an IACS asset in the Cell/Area Zone currently classified as a Level_1_Controller needs to be accessed by the remote desktop server in the Industrial Zone. The current policy is that no IACS asset can be accessed by the remote desktop server unless the IACS asset is classified as Remote_Access. To allow this remote access, the asset's Security Group Tag (SGT) must be updated by a Change of Authorization (CoA). To initiate the update, the custom attribute must be updated by changing the Group value for the asset in Cisco Cyber Vision. The change is propagated over pxGrid and the device is reprofiled. Based on the updated attribute, ISE determines that the endpoint should be profiled as Remote_Access. When the device is profiled as Remote_Access, ISE sends a CoA (CoA type based on the configured "Associated CoA Type" setting (Port Bounce, Reauth, or Global Setting) for that profile. The CoA is sent to the network device which will signal the network device to Port Bounce or Reauthenticate the port where the IACS asset is connected. Upon reauthenticating with ISE, the device should satisfy a different authorization rule which applies the Remote_Access SGT. Figure 31 illustrates the profiling policy used to match Remote_Access.

Note: When a new SGT is assigned to an IACS asset, there is a loss of connectivity for a few seconds, during which time no application is able to access the IACS asset.

Figure 31 Profiling Rule for Remote Access

Configuring TrustSec in Cisco ISE

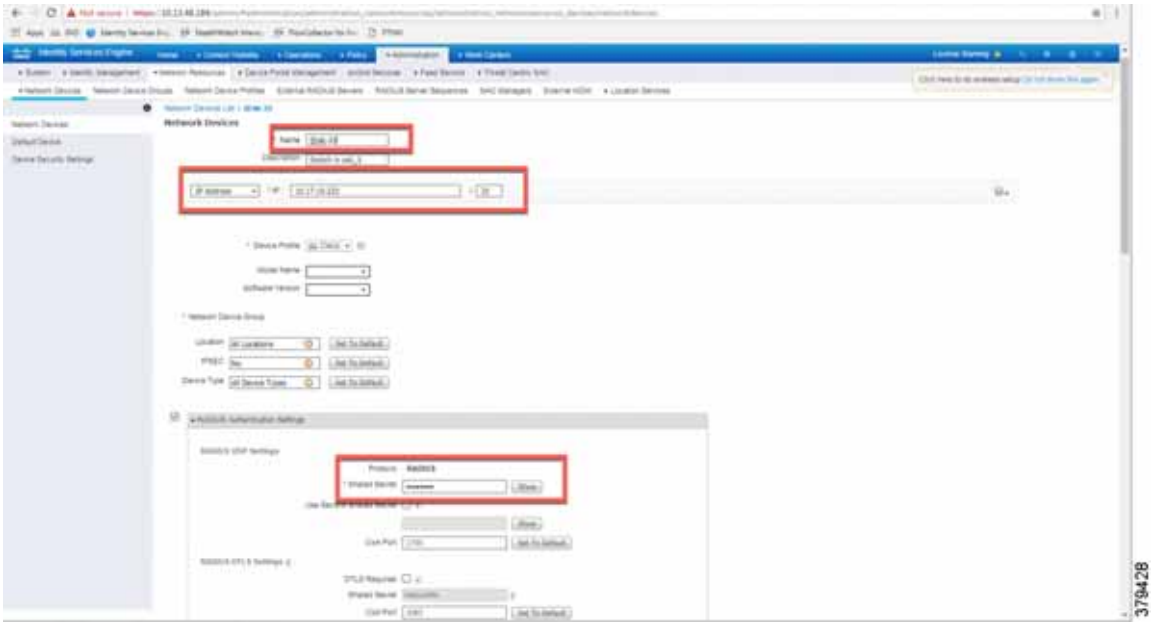
This section provides configuration details for TrustSec communication between ISE and networking devices.

- Adding switches to Cisco ISE
- Configuring Security Group Tag Exchange Protocol (SXP)
- Configuring Authentication Policies
- Configuring Authorization Policies
- Adding SGTs
- Configuring TrustSec Policy Matrix

Adding Switches to Cisco ISE

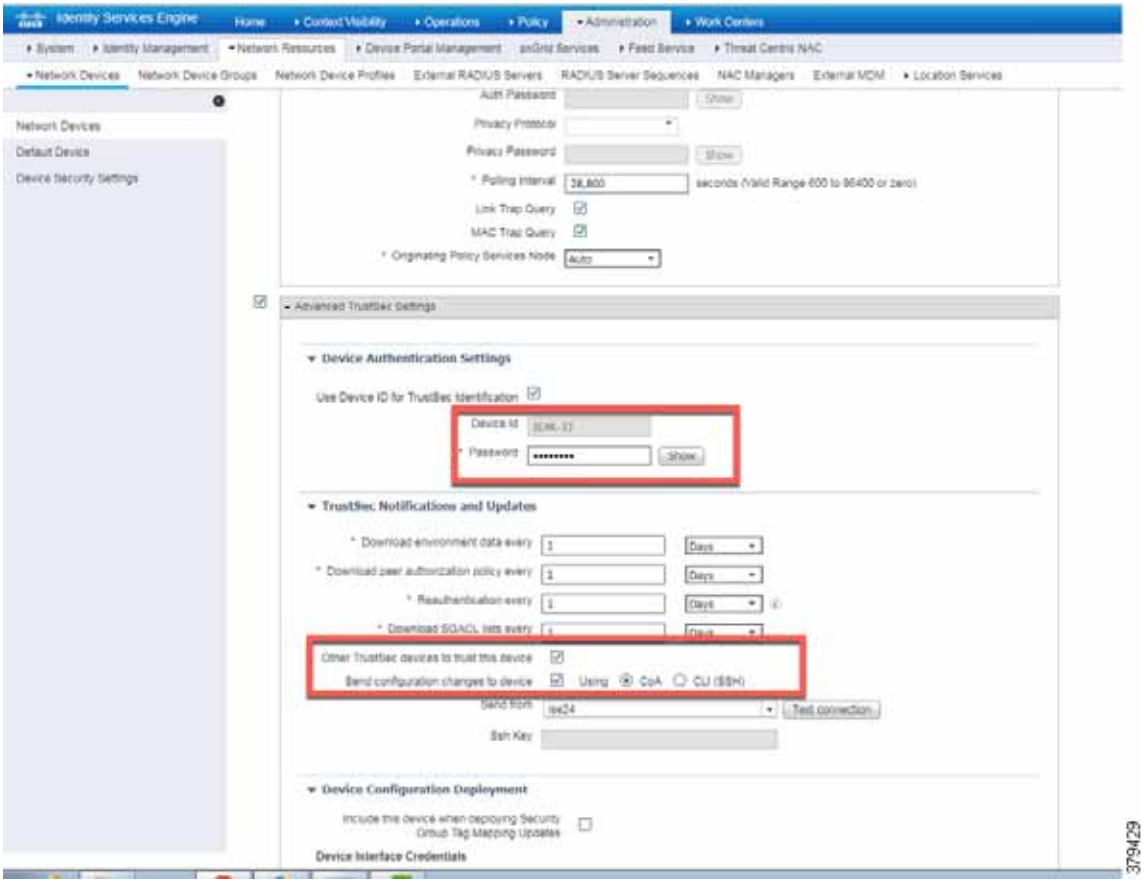
For Cisco ISE to assign SGTs to IACS assets, switch details such as the IP address and RADIUS pre-shared secret key must be defined in Cisco ISE. From the ISE web UI, navigate to **Administration –>Network Resources -> Network Devices** to configure device details. Figure 32 shows the information needed to establish a successful RADIUS connection Cisco ISE and a switch.

Figure 32 RADIUS Configuration



Details must also be configured for TrustSec updates, as shown in Figure 33.

Figure 33 CTS Configuration for IES



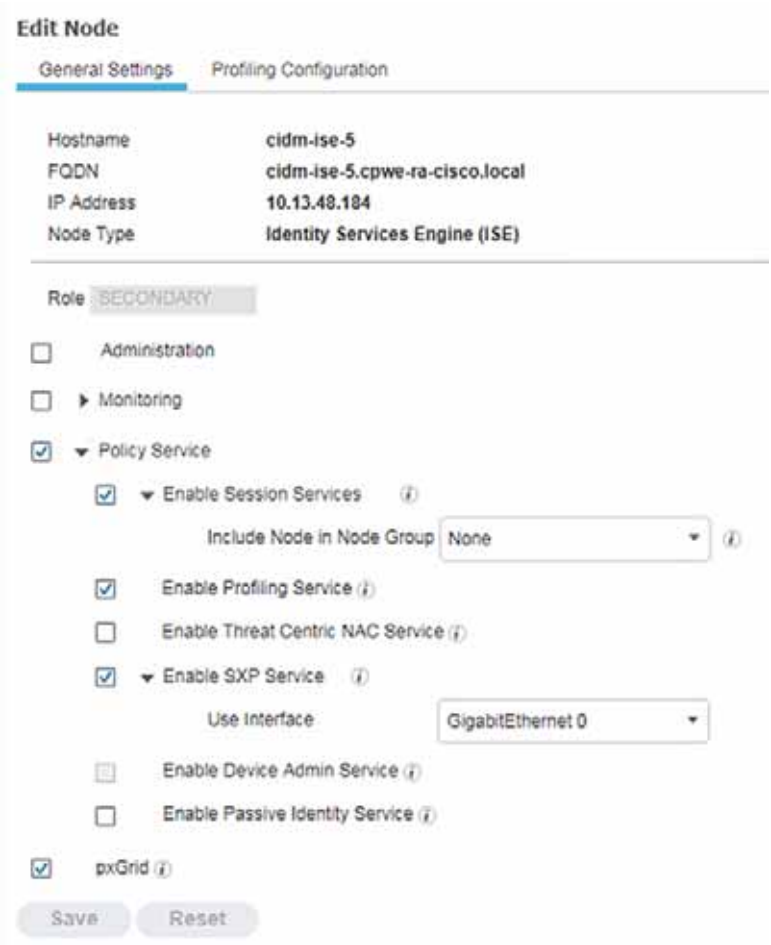
Configuring SXP in Cisco ISE

This section describes how to enable SXP and configure SXP peers in Cisco ISE.

Enabling SXP Service in Cisco ISE

The SXP service must be enabled on the PSN. From the ISE web UI, navigate to **Administration -> System -> Deployment**. Check the check box for the appropriate PSN and click **Edit**. Under **General Settings**, check the **Enable SXP Service** check box and then click **Save**.

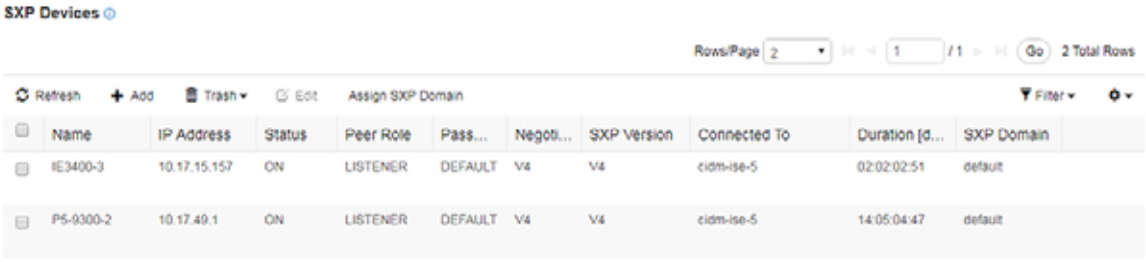
Figure 34 Enabling SXP Service in Cisco ISE



Configuring SXP Peers

SXP allows ISE and access devices to pass SGT information across networking devices that do not support inline tagging. For the Cell/Area Zone, the distribution switch is configured as the Listener, and Cisco ISE is enabled as a Speaker. To configure SXP, from the ISE web UI navigate to **Work Centers –> TrustSec -> SXP**.

Figure 35 Configuring SXP Peers in Cisco ISE



Configuring Authentication Policies

802.1x authentication policy involves three parties:

- The supplicant—A client device that wishes to attach to the network.
- The authenticator—A networking device that accepts authentication requests from the client and sends them to the RADIUS authentication server.
- The authentication server—The device that validates a client's identity and sends back the success or failure RADIUS message.

In this CVD, the supplicant is the IACS asset, the authenticator is the Cisco IE switch, and the authentication server is an ISE node configured with the Policy Service Node (PSN) persona.

Authentication policies are used to define the protocols used by Cisco ISE to communicate with the IACS assets and the identity sources to be used for authentication. Cisco ISE evaluates the conditionsand applies the respective access. The authentication protocol tested in this CVD s called MAC Authentication Bypass (MAB). MAB uses the MAC address of a device to determine what kind of network access to provide. This protocol is used to authenticate end devices that do not support 802.1x.

For more information about MAB, see:
https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-services/config_guide_c17-663759.html

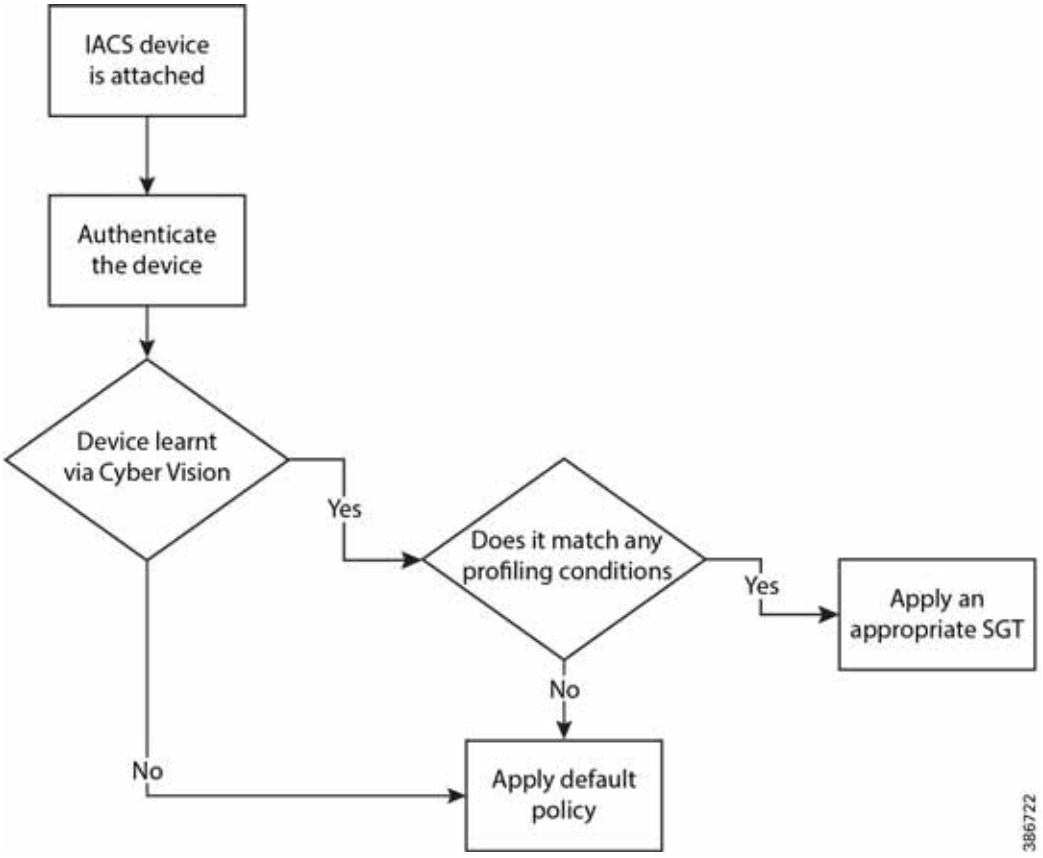
The authentication policy used in the Cisco ISE for this CVD checks wired or wireless MAB is being used and that the endpoint is present in the Internal Endpoints identity store. To configure the authentication policy, navigate to **Policy -> Policy Sets**. For the **Default** Policy Set, click the arrow button under the **View** column, as shown in Figure 38.

Configuring Authorization Policies

Authorization policies are critical to determine what a user or device is allowed to access within the network. Authorization policies are a set of rules. Each rule contains one or more conditions and a set of pre-defined results to be applied when the conditions are met. In ISE, the result of a rule is called an Authorization Profile.

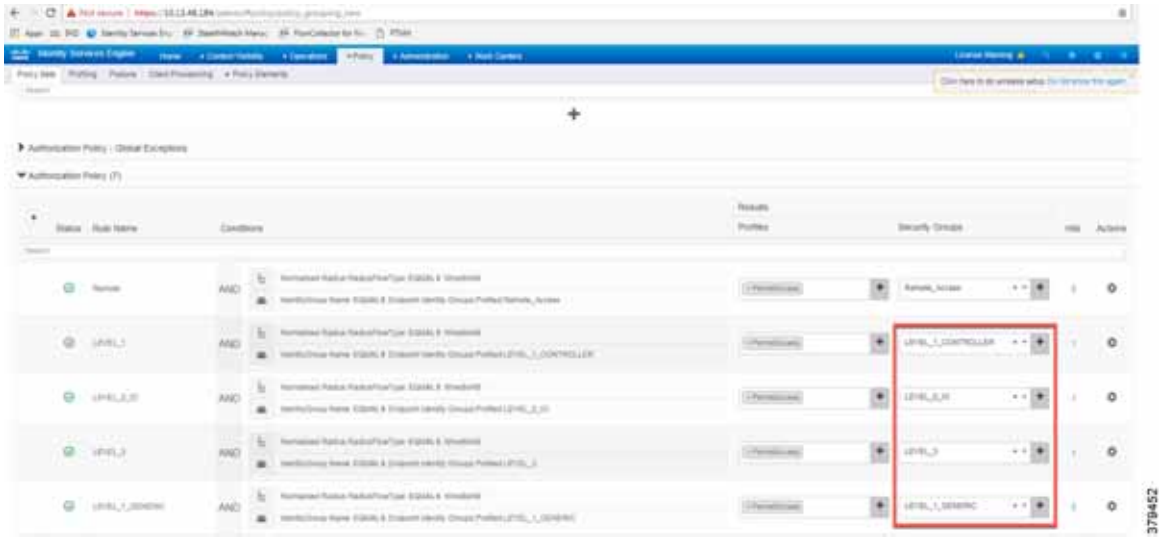
Authorization profiles group the specific permissions granted to a user or a device and can include attributes such as an associated VLAN, Downlloadable ACL, or SGT. This CVD uses SGT to grant permissions to an IACS asset. Configuring TrustSec Policy Matrix, page 42 describes how the Policy Matrix was designed. When an IACS asset is authenticated it is matched to an authorization policy which assigns the appropriate SGT to the asset. The TrustSec Policy Matrix determines the permissions associated with each SGT. Figure 36 shows the high-level steps when an IACS asset is connected to the network. To configure the authorization policy, navigate to **Policy -> Policy Sets**. For the **Default** policy set, click the arrow button in the **View** column. Click the **Authorization Policy** button to expand the authorization rules.

Figure 36 AAA for an IACS Asset



The authorization rules can be tailored to fit varying security policies; much like ACLs, there can be a default rule to apply if no other rules match and that rule can give basic or no access. Figure 37 shows the authorization policies for this CVD.

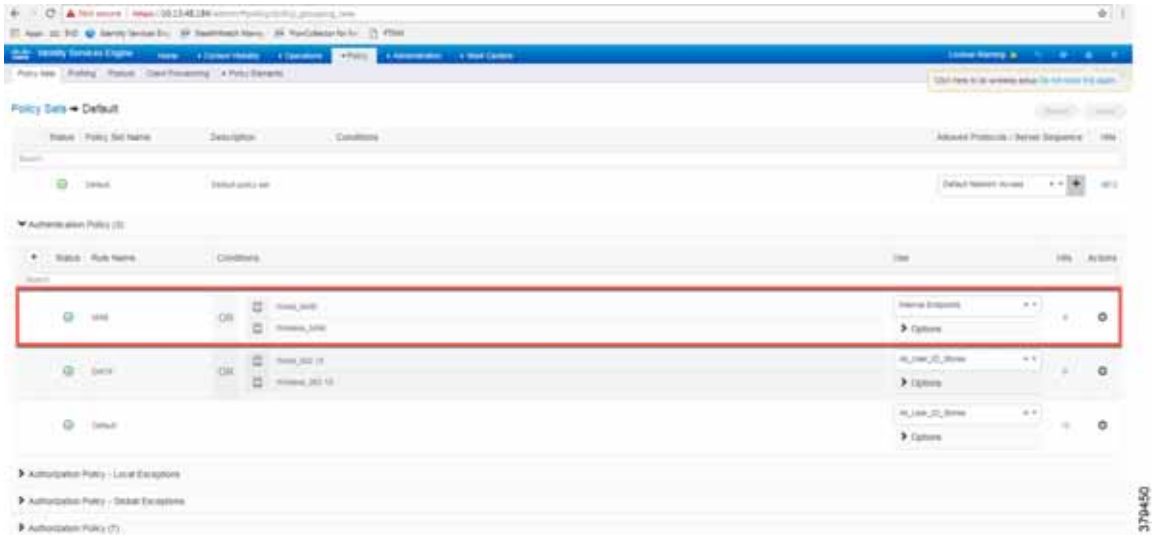
Figure 37 Authorization Policy Conditions



Note: In the example shown in Figure 39, the default authentication policy set was used. In case the real deployment has a different authentication policy set, then the IT Security Architect must select the correct authentication policy set.

Figure 38 Navigation to Configure Authentication/Authorization Policy

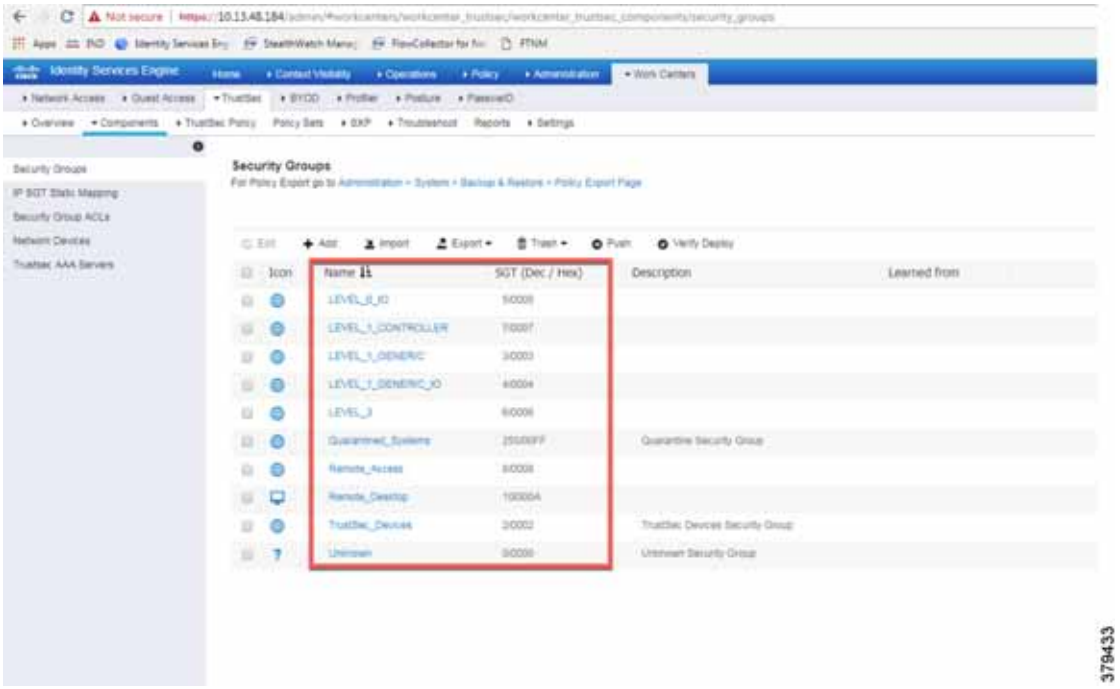
Figure 39 ISE Authentication Policy



Configuring SGT Components

Once an IACS asset is profiled, it is matched to an authorization policy which assigns an SGT to the device. Figure 40 shows an example of SGTs created in Cisco ISE to segment the network, which is located at **Work Centers –> TrustSec –> Components**.

Figure 40 Configuring SGT Components in Cisco ISE



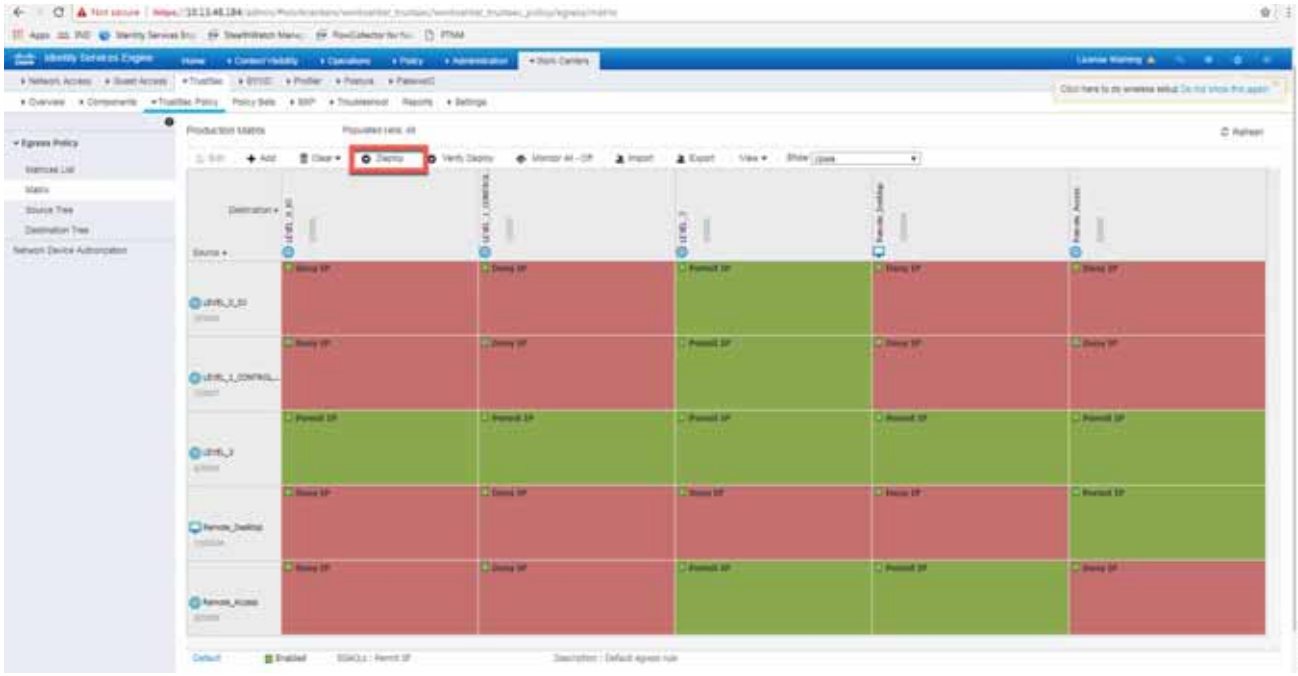
Configuring TrustSec Policy Matrix

This section describes how to design a policy matrix for Cisco ISE. Based on the example illustrated in Table 3, the following are policy matrix rules:

- IACS assets or any other devices that are assigned with the SGT group of Level_3 are allowed to access all the devices in the plant-wide network.
- IACS assets with SGT value of Level_1_Controller are allowed to access only the devices in the same Cell/Area Zone.
- IACS assets with SGT value of Level_0_IO are allowed to access only the devices in the same Cell/Area Zone.
- IACS assets with Remote_Access are allowed to communicate with another device assigned with SGT value of Remote_Desktop and Level_3 (because Level_3 has access to all the devices).

Figure 41 shows the TrustSec Access Policy Matrix.

Figure 41 TrustSec Access Policy Matrix



As shown in Figure 41, a Level_3 controller is allowed to communicate with all the IACS assets, however Level_1_Controller and Level_0_IO can only communicate if they are present in the same Cell/Area Zone. After defining the TrustSec Policy in the ISE, it is downloaded to all networking devices by clicking **Deploy**, as shown in Figure 41.

Access Level Switch Configuration

This section provides the configuration details for the Cisco IE switches in the Cell/Area Zone. The configuration of key features, such as TrustSec, NetFlow, and RADIUS, are described below.

Configuring RADIUS AAA

Each switch must be configured to communicate with the Cisco ISE AAA server for authorizing IoT devices, users, and other systems. The AAA server shown in this configuration is pointing to the ISE PSN. The following configurations are performed via the switch CLI.

1. In configuration mode, designate the switch source interface or VLAN that will be used to communicate with the ISE PSN.

   ```
   ip radius source-interface interface_number
   ```

2. Configure AAA parameters and the AAA group name.

   ```
   aaa new-model
   aaa group server radius ISE
    server name ISE

   aaa authentication login no-auth none
   aaa authentication dot1x default group ISE
   aaa authorization network cts-list group ISE
   aaa authorization auth-proxy default group ISE
   aaa accounting dot1x default start-stop group ISE
   aaa session-id common
   ```

3. Configure Change of Authorization (CoA):

```
aaa server radius dynamic-author
client PSN_IP_ADDRESS server-key 7 SHARED_KEY
!
```

Note: This configuration must match the configuration done on Cisco ISE. Refer to Figure 37.

4. Configure the RADIUS server for TrustSec. The list name should be tied to the **aaa authorization network** command shown in Step 2:

```
cts authorization list cts-list
!
```

5. Configure the following RADIUS server attributes:

```
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server dead-criteria time 5 tries 3
!
```

6. Configure the RADIUS server, IP address, and shared secret that was entered in Cisco ISE:

```
radius server ISE
address ipv4 PSN_IP_ADDRESS auth-port 1812 acct-port 1813 pac key 7 PAC_KEY
!
```

7. Globally enable port-based authentication:

```
dot1x system-auth-control
!
```

Configuring Port-based Authentication

On the access switch, the following configurations enable port-based authentication. Configure each interface that will have an endpoint device connected. For MAB and Dot1x methods to co-exist and function as expected, the order and priority must be properly specified as referenced in this application note Configuring MAB: http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-service/application_note_c27-573287.html

In this CVD, the **authentication open** command was applied to the port to ensure that the device remains connected even if the port is unable to authenticate to the RADIUS server.

```
!
interface GigabitEthernet1/10
 description Connected to a Controller
 switchport access vlan 101
 switchport mode access
 ip flow monitor StealthWatch_Monitor input
 load-interval 30
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication open
 authentication order mab dot1x
 authentication priority mab dot1x
 authentication port-control auto
 authentication periodic
 authentication timer reauthenticate server
 mab
 snmp trap mac-notification change added
 snmp trap mac-notification change removed
 dot1x pae authenticator
 dot1x timeout tx-period 10
 spanning-tree portfast edge
!
```

Configuring SDM Templates

SDM templates will allow an OT control system engineer to prioritize resources for different features enabled on an IE switch. In this CVD, the routing template is required to support SGT assignment.

```
sdm prefer routing
```

After entering the command, the IE switch must be rebooted.

Configuring CTS Credentials

Specify the Cisco TrustSec device ID and password for the switch to use when authenticating with Cisco ISE and establishing the PAC file. This password and ID must match the Cisco ISE Network Devices configuration for the respective switch.

```
cts credentials id switch ID password password
```

Configuring NetFlow

The NetFlow configuration has three components: Flow Record, Flow Exporter, and Flow Monitor. After the three components (explained below) have been configured, the Flow Monitor is applied to a physical interface.

Flow Record

A Flow Record defines the information that will be gathered by the NetFlow process, such as packets in the flow and the types of counters gathered per flow. Custom flow records specify a series of **match** and **collect** commands that the switch includes in the outgoing NetFlow record.

The match fields are the key fields, meaning that they are used to determine the uniqueness of the flow. The collect fields are extra information that is included in the record in order to provide more detail to the collector for reporting and analysis. When a Flow Record is defined, all of the flow data traffic that enters (ingress) or leaves (egress) the device is captured.

This configuration example includes required as well as optional flow record fields needed by Stealthwatch.

```
flow record StealthWatch_Record
description NetFlow record format to send to StealthWatch
match datalink mac source address input
match datalink mac destination address input
match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect transport tcp flags
collect interface input
collect interface output
collect flow cts source group-tag
collect flow cts destination group-tag
collect counter bytes long
collect counter packets long
collect timestamp sys-uptime first
collect timestamp sys-uptime last
```

Flow Exporter

The Flow Exporter defines where and how to send the NetFlow records. The Exporter configuration defines a recipient IP address and port; in this CVD the Stealthwatch Flow Collector is the destination.

```
flow exporter StealthWatch_Exporter
 description StealthWatch Flow Exporter
 destination 10.13.48.183
 source Vlan101
 output-features
 transport udp 2055
 template data timeout 60
 option application-table
!
```

Flow Monitor

A Flow Monitor defines the NetFlow cache timeout parameters, as well as linking the Flow Record with the Flow Exporter. As network traffic traverses the Cisco device, flows are continuously created and tracked. As the flows expire, they are exported from the NetFlow cache to the Stealthwatch Flow Collector. A flow is ready for export when it is inactive for a certain time (for example, no new packets received for the flow) or if the flow is long-lived (active) and lasts greater than the active timer (for example, long FTP download and standard CIP I/O connections).

1. Configure the Flow Monitor:

```
flow monitor StealthWatch_Monitor
 description StealthWatch Flow Monitor
 exporter StealthWatch_Exporter
 cache timeout active 60
 cache timeout update 5
 record StealthWatch_Record
!
```

2. Once the flow monitor has been created, it can be applied to switch interfaces. In this example we apply the Flow Monitor on the ingress traffic, as denoted by the **input** keyword:

```
!
interface GigabitEthernet1/10
 description Connected to a Controller
 switchport access vlan 101
 switchport mode access
 ip flow monitor StealthWatch_Monitor input
```

Configuring Distribution Switch—Cisco Catalyst 9300

As described in the design guide, TrustSec enforcement is applied at the distribution switch (Catalyst 9300). The RADIUS and CTS configurations for the Catalyst 9300 follow the same guidelines as the IE switch configurations. Three additional TrustSec features are required for the distribution switch:

- IP device tracking (IPDT)
- SXP tunnel
- Enforcement

Configuring IPDT

On the Cisco Catalyst 9300, the device tracking feature must be enabled, a device tracking policy must be created, and this policy must be applied to the interface where the IP device tracking needs to be enabled. In this CVD, IP device tracking is enabled on interfaces connected to access switches.

```
device-tracking tracking
!
device-tracking policy IPDT
 no protocol udp
 tracking enable
!
interface Port-channel3
```

```
 switchport trunk native vlan 101
 switchport trunk allowed vlan 101,102
 switchport mode trunk
 device-tracking attach-policy IPDT
end
```

Configuring SXP Tunnel

The SXP tunnel between the distribution switch and ISE must be established to populate the distribution switch with endpoint SGT information for enforcement.

```
cts sxp enable
cts sxp default password 7 shared key
cts sxp connection peer PSN_IP_ADDRESS source SWITCH_IP_ADDRESS password default mode local speaker
hold-time 0
```

Enforcement

To enable policy enforcement, enter the following commands:

```
cts role-based enforcement
cts role-based enforcement vlan-list vlan-id
```

Cisco Cyber Vision Center Configuration

Installation

For this implementation, the Cisco Cyber Vision Center was deployed as a VM in the Level 3 Site Operations Zone. For VM installation instructions refer to: https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_Center_VM_Installation_Guide_Release_3_0_1.pdf.

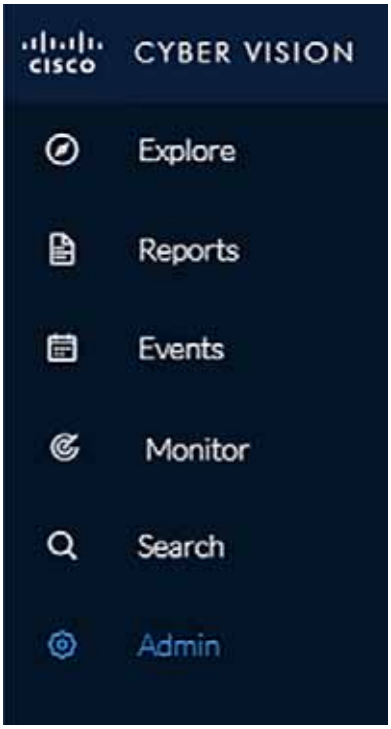
Cisco Cyber Vision Center Interfaces

The Cisco Cyber Vision Center system has two interfaces: eth0 and eth1. Eth0 is used for web UI access as well as pxGrid communication. Eth1 is used for Cisco Cyber Vision Sensor communication. Therefore, appropriate network settings should be configured to suit these communication schemes. Please refer to the installation guide for the configuration of these interfaces.

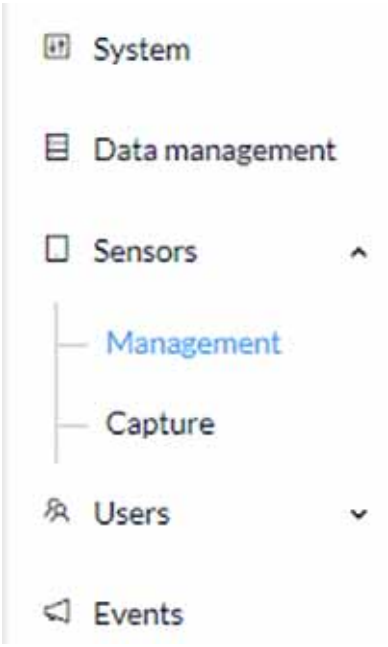
Joining Sensors to Cisco Cyber Vision Center

The Cisco Cyber Vision Sensors provide all of the monitored traffic to the Cisco Cyber Vision Center for user analysis, and they securely communicate with the Cisco Cyber Vision Center using trusted certificates. To connect the Cisco Cyber Vision Sensors to the Cisco Cyber Vision Center, do the following:

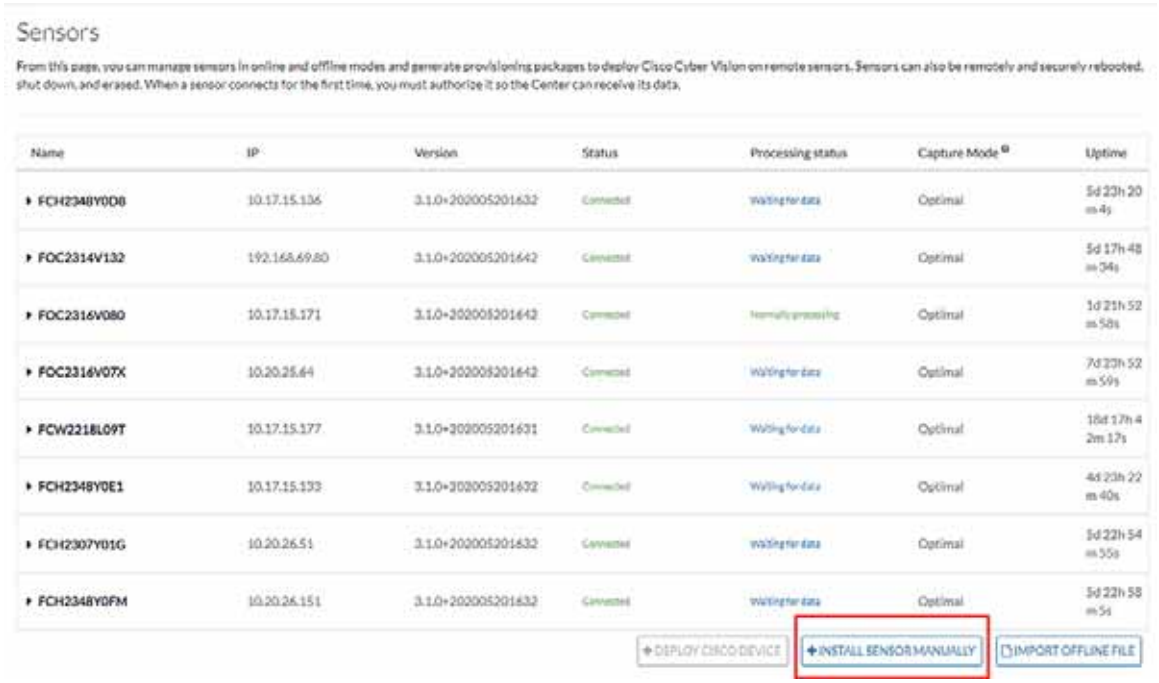
1. From the Cisco Cyber Vision Center web UI, choose **Admin** on the left menu pane.



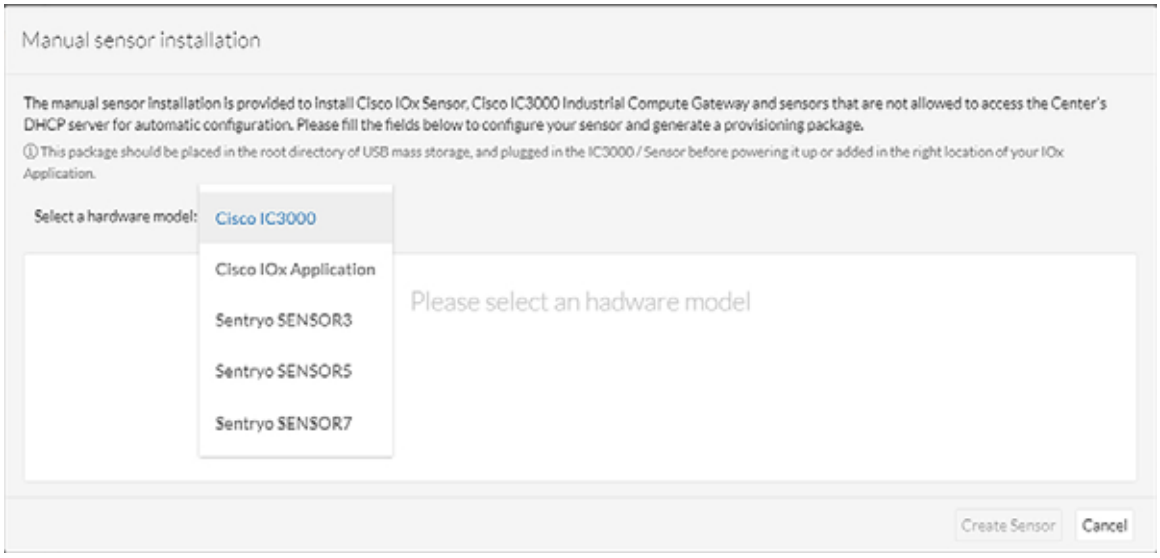
2. Choose **Sensors** from the **Admin** menu. By default, it will load the **Management** page.



3. Click the **Install Sensor Manually** button at the bottom of the **Sensors** list.



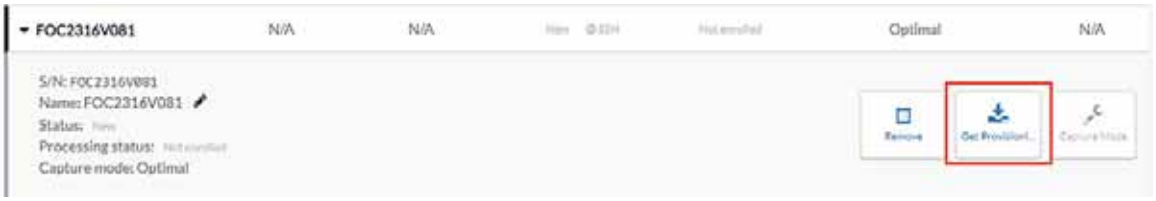
4. Select a hardware model from the **Hardware Model** drop-down list. The resulting configuration options will be different for each device type.



5. Enter the required information, such as serial number, IP address of the Cisco Cyber Vision Center for the Cisco Cyber Vision Sensor to use, and so on. The IC3000 will require network configuration for both the IC3000 Local Manager and the Cisco Cyber Vision Sensor application.

6. After entering the details, click the **Create Sensor** button.

7. On the **Sensors** page, click the newly created sensor to expand for more details. Click the **Get Provisioning Package** button to download the zipped files to be used in configuring the sensor. This package includes certificate, password, network, and other configuration details.

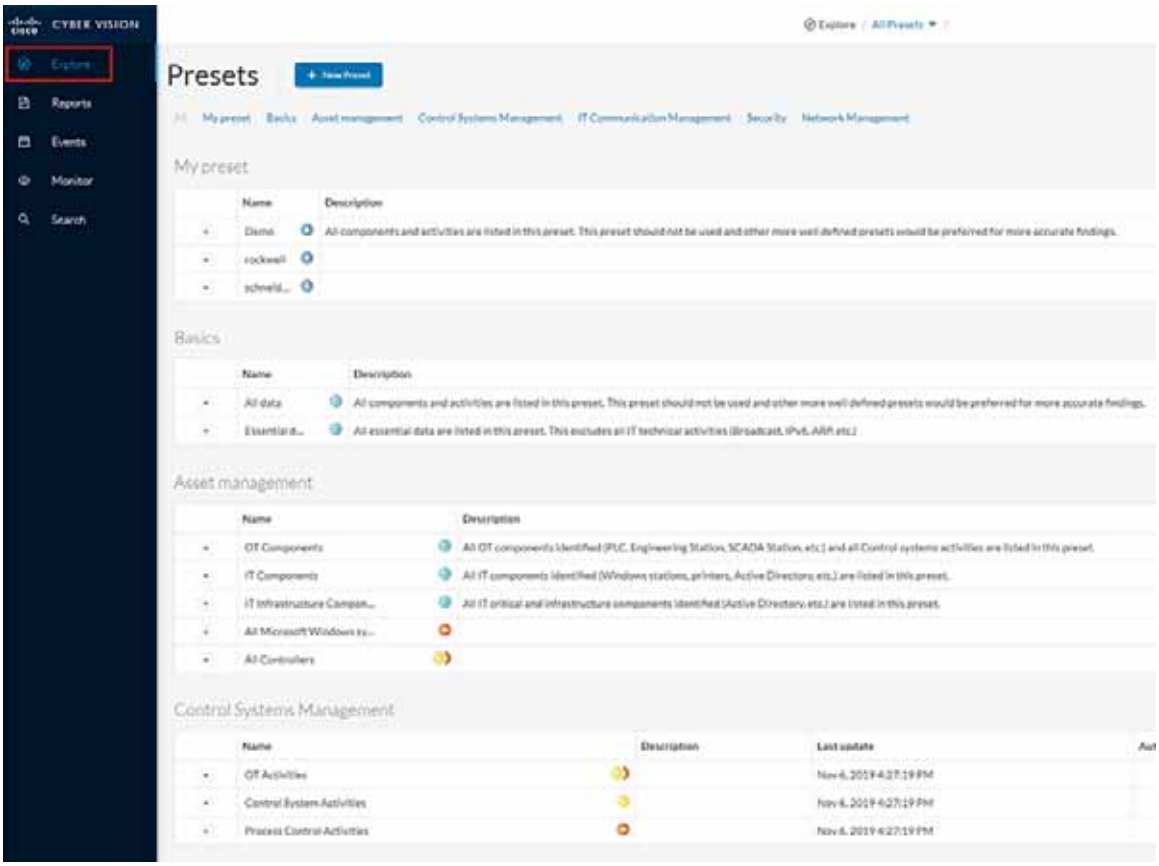


8. Once subsequent sensor installation procedures are complete, the **Status** column on the **Sensors** page will show the newly installed sensor as “Connected”.

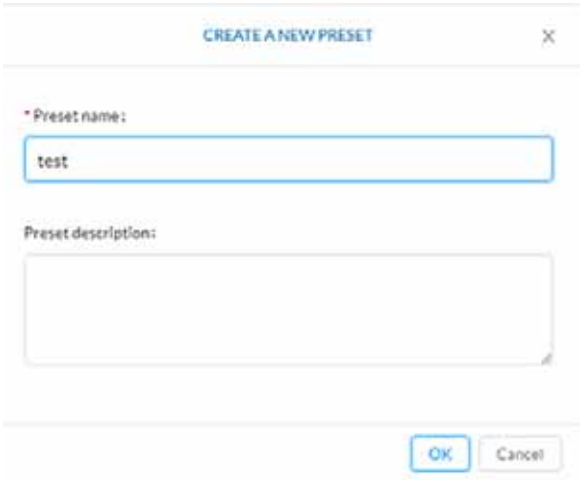
Configuring Presets

Presets allow the user to customize how components are displayed and grouped. In addition, the presets allow the user to quickly navigate to device activity, vulnerability, and event information. The Cisco Cyber Vision Center comes with default presets, such as Control Systems Management, but the user can create their own by doing the following:

1. Choose **Explore** in the left menu pane to display all of the current presets:

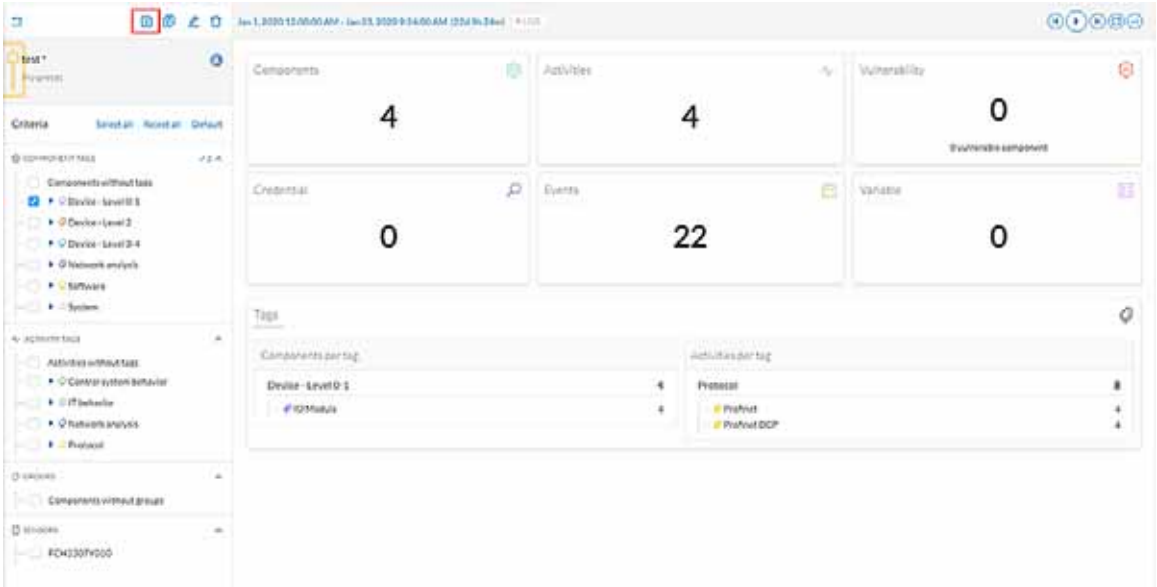


2. At the top, click the **New Preset** button. Provide a name and an optional description:



3. The new preset will now show in the **My preset** list. Click the icon next to the preset name to configure the preset options:

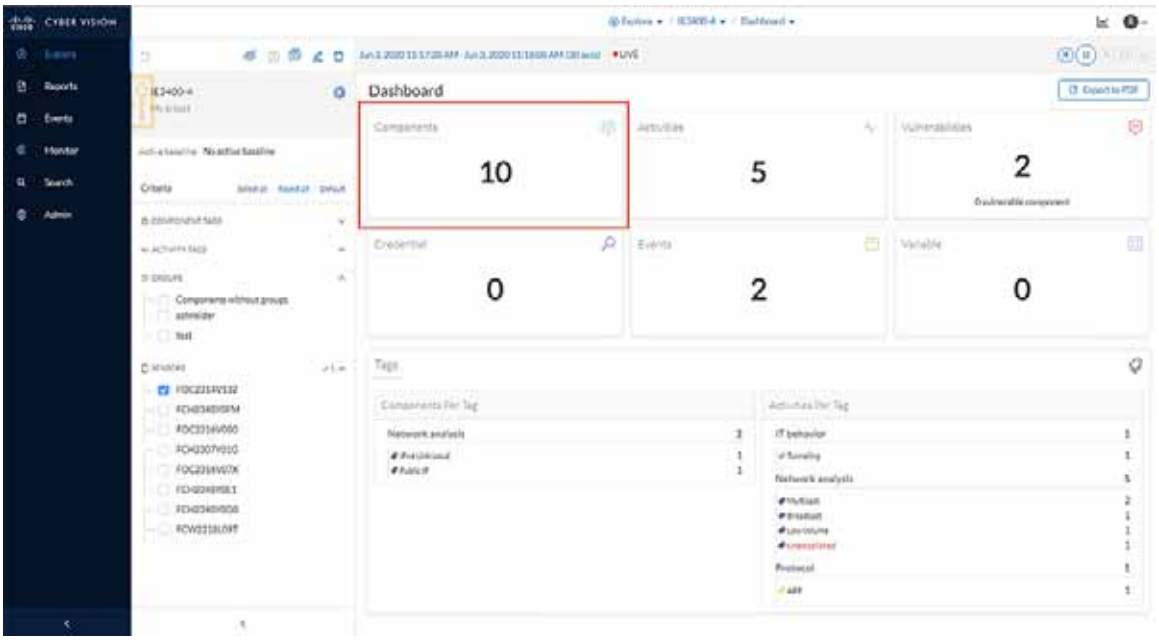
4. Select desired preset criteria and click the icon above the preset name to save the changes:



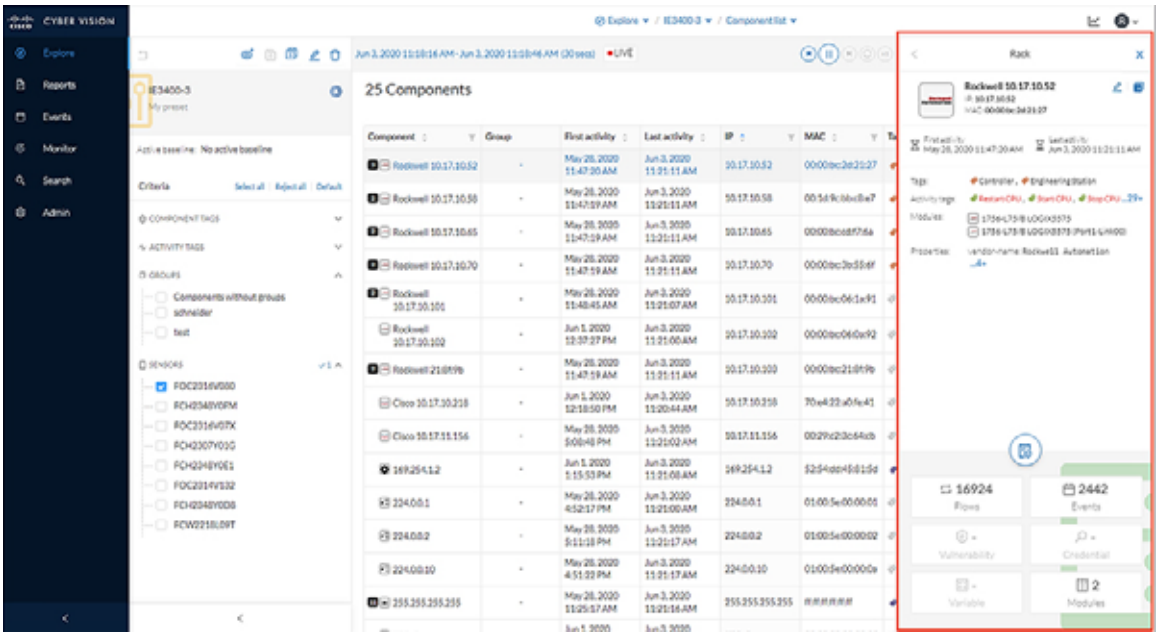
Viewing Assets

As described in the previous section, Presets allow the user to view specific components and their details based on saved filters. To view a list of assets from a Preset, do the following:

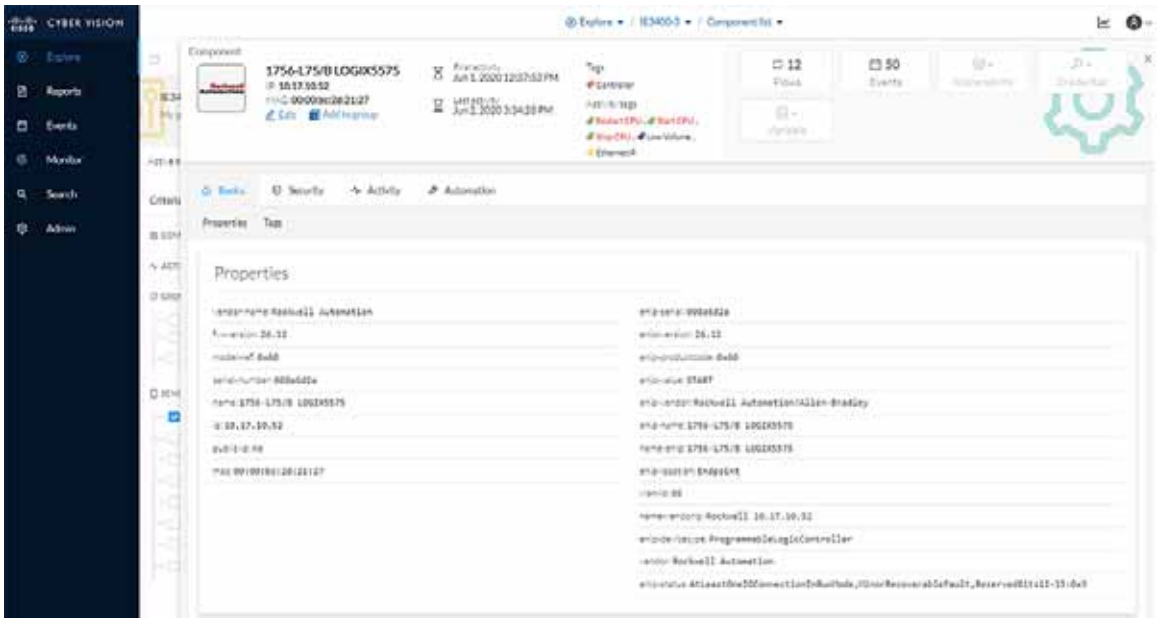
1. Choose **Explore** in the left menu pane to display all of the current presets.
2. Click the name of the desired Preset.
3. From the **Dashboard** pane, click the **Components** button.



4. The list of components matching the Preset criteria will be displayed in a list. Clicking one of the components will load a pane on the right displaying more details.



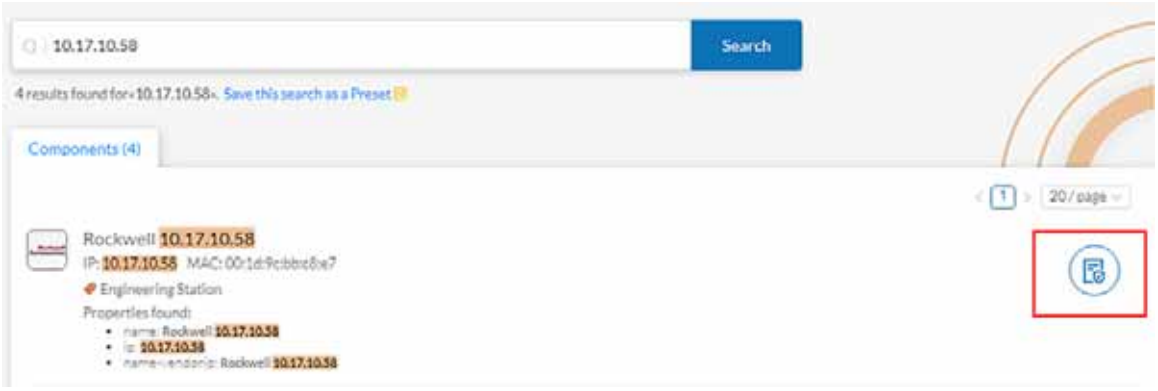
5. Click the **Technical Sheet** icon to give asset attributes such as vendor, model, device type, and more.



The **Search** option on the left pane can also be used to display component details.

1. In the **Asset Search** field, enter an IP address, MAC address, or other device attribute.

2. By hovering over the desired result, the **Technical Sheet** icon appears on the right. Click the icon to view the asset details.



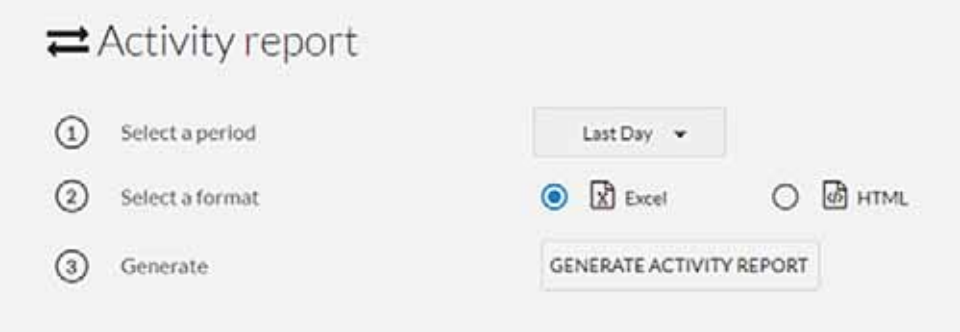
Viewing Asset Activity

Asset activity can be viewed in two ways: Reports and Presets.

An activity report includes asset flow information, highlighting communication between devices with details such as IP addresses, ports, and tags. To view an activity report, do the following:

1. Click the **Reports** option in the left menu pane, and click the **Activity report** button:

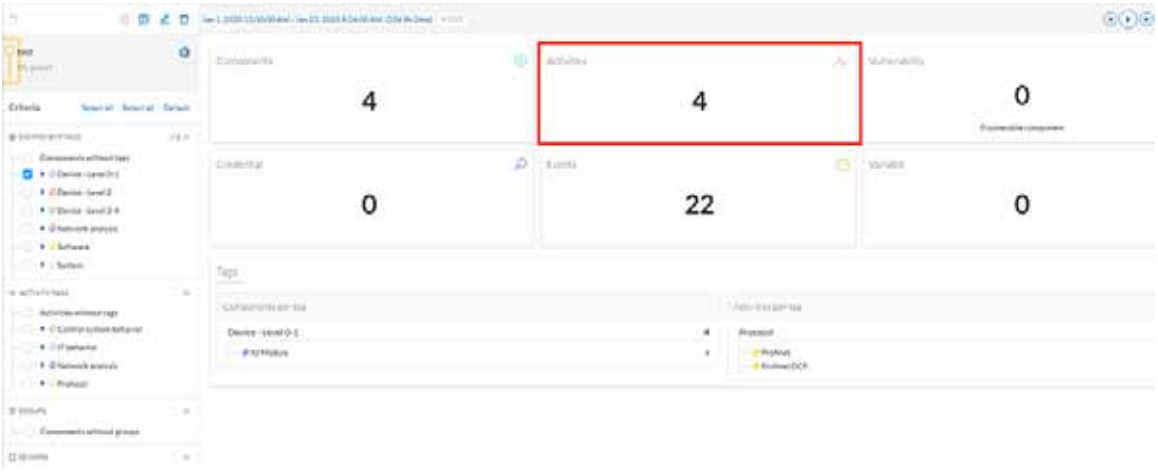
2. Choose a time range for the activity and select an output format:



3. The generated report will show in the **History** pane for the user to download

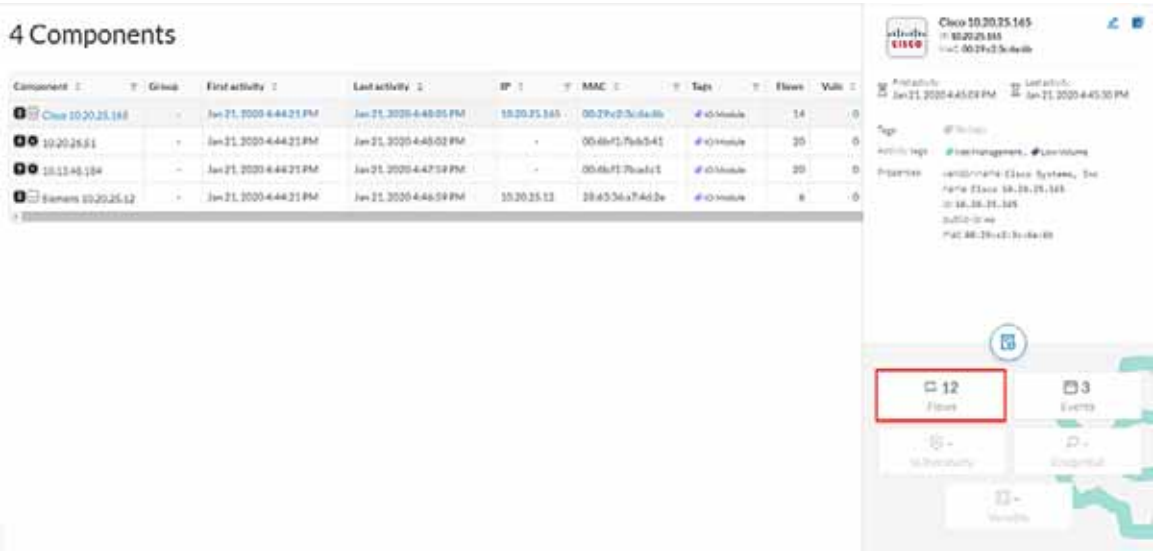
The second way to view activity is to use Presets, which allows the user to look at specific assets. To view activity for a particular device or all devices in a Preset, do the following:

1. Click the **Explore** option in the left menu pane to display all of the current Presets. Click the icon next to the desired Preset name. To view activity for all devices included in the Preset, click the **Activities** button:

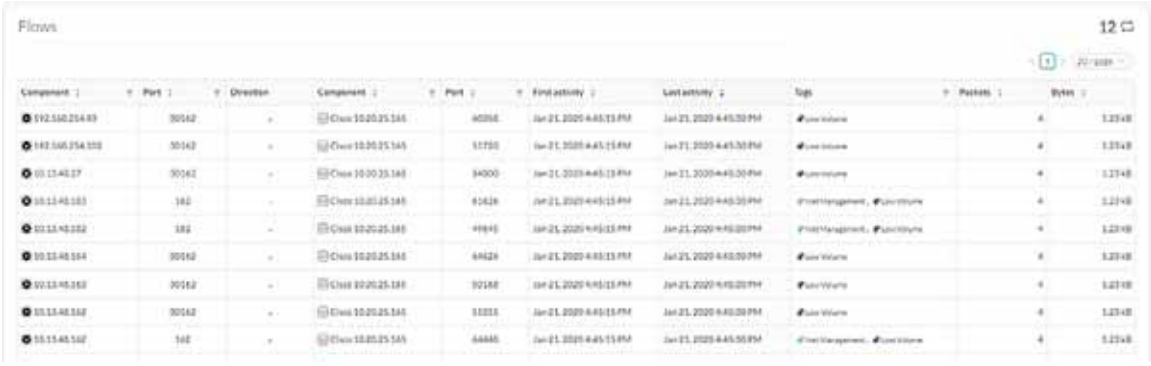


2. A table will be displayed showing the communication flows between devices, including time frames and any events associated with the communication.

3. Alternatively, clicking the **Components** button in the preset window will display all devices included in that preset. Select a component and choose the **Flows** button in the pane on the right:



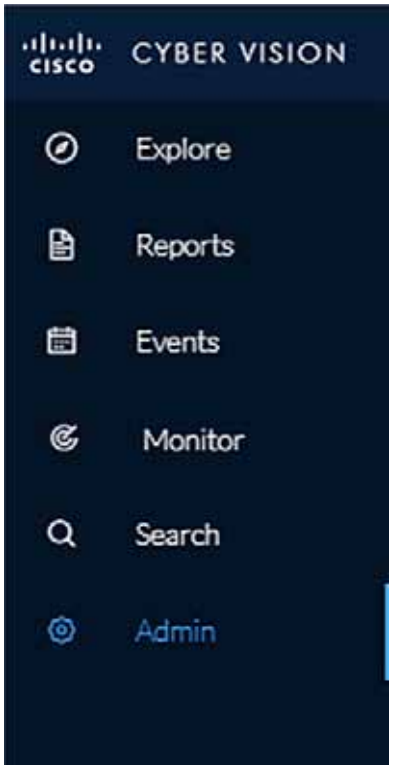
4. A table showing the activity information will be displayed:



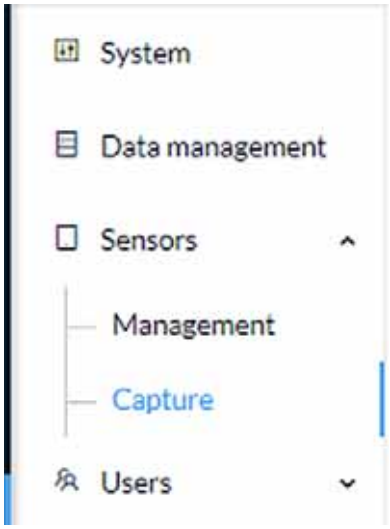
Performing a Packet Capture on a Sensor

The packet capture feature is useful for both troubleshooting data propagation issues and retrieving underlying details of network communications for investigation purposes. To perform a packet capture on a Cisco Cyber Vision Sensor, do the following:

1. From the Cisco Cyber Vision Center web UI, choose **Admin** on the left menu pane.

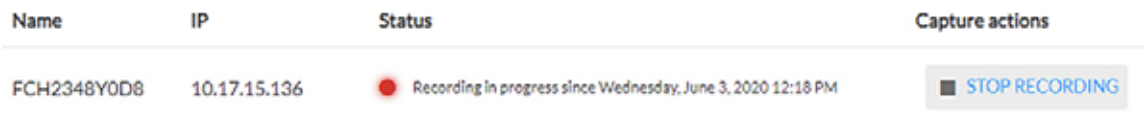


2. Choose **Sensors** from the **Admin** menu, then choose **Capture** from the submenu.



3. Click the **Start Recording** link for the desired sensor.

While it is recording, the **Status** column indicates the recording activity with a red icon.



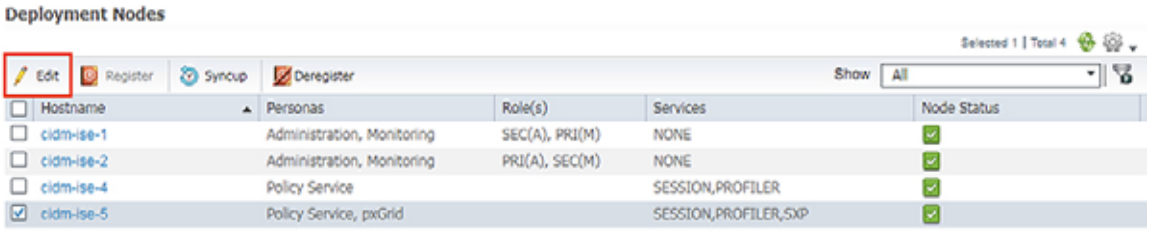
4. Click the **Stop Recording** link in the **Capture Actions** column after the desired amount of time has elapsed.
5. A **Download** link will appear for the desired sensor. Clicking this link will initiate download of the packet capture file.

Integrating Cisco Cyber Vision Center with Cisco ISE pxGrid

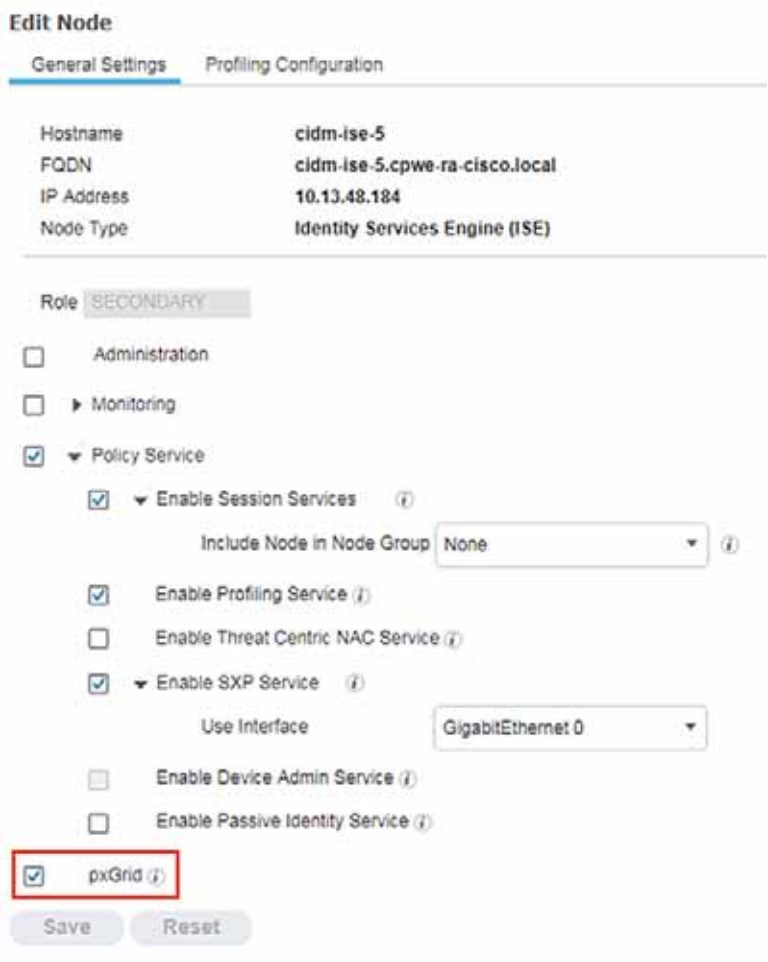
Cisco Cyber Vision Center can share several asset details with ISE using the pxGrid feature. These attributes provide context for more accurate profiling of devices, which further enhances the TrustSec scheme in the architecture. Cisco Cyber Vision Center and ISE communicate securely by exchanging certificates. To configure the pxGrid connection, do the following:

Enable pxGrid in ISE

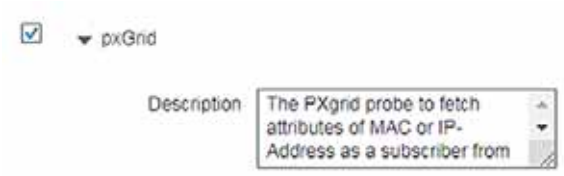
1. In the ISE web UI, navigate to **Administration -> System -> Deployment**. Check the box next to the appropriate PSN and click the **Edit** button.



2. Under the **General Settings** tab, check the **pxGrid** checkbox.



3. Under the **Profiling Configuration** tab, check the **pxGrid** checkbox.



Download the Cisco Cyber Vision Center Certificate

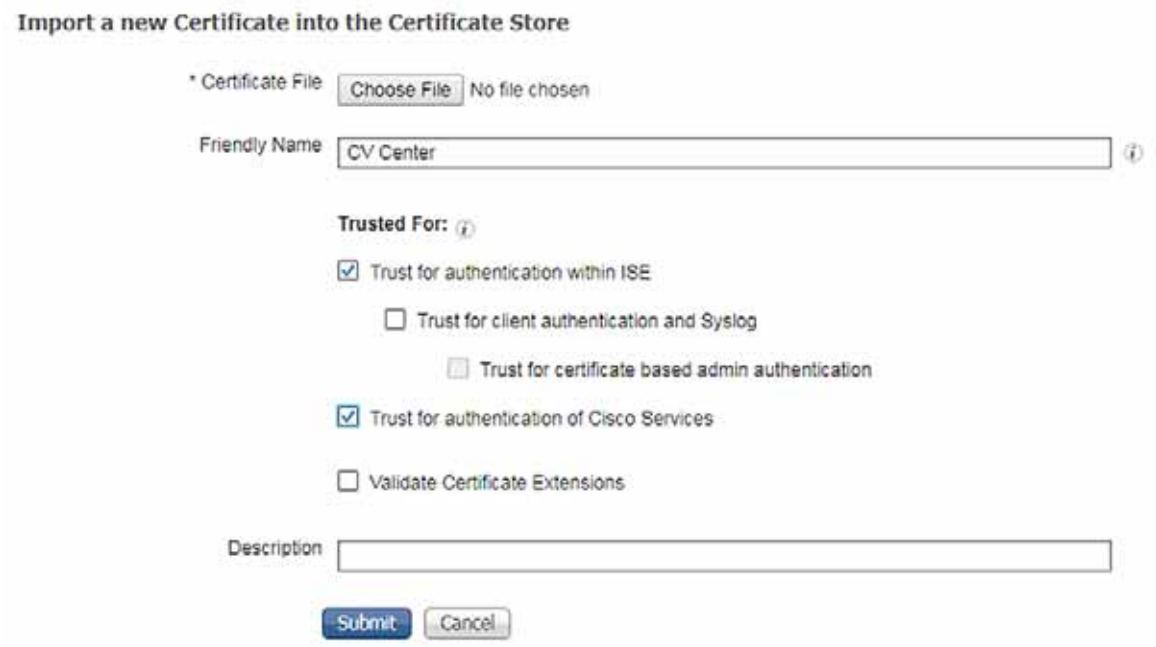
1. From the Cisco Cyber Vision Center web UI, choose **Admin** on the left menu pane.
2. Choose **PxGrid** from the **Admin** menu.

3. Click the **Download Certificate** button.

Import the Cisco Cyber Vision Center Certificate into ISE

1. In the ISE web UI, navigate to **Administration -> System -> Certificates -> Trusted Certificates**.
2. Click the **Import** button.

3. Click the **Choose File** button to upload the Cisco Cyber Vision Center certificate.
4. Enter a **Friendly Name** if desired, and check the **Trust for authentication within ISE** and **Trust for authentication of Cisco Services** check boxes. Click the **Submit** button when finished.



Generate a pxGrid Certificate for Cisco Cyber Vision Center

1. In the ISE web UI, navigate to **Administration -> pxGrid Services -> Certificates**.

2. From the **I want to** drop-down list, choose **Generate a single certificate (without a certificate signing request)**.
3. In the **Common Name (CN)** field, enter a name to indicate this certificate is used for Cisco Cyber Vision Center.
4. From the **Subject Alternative (SAN)** drop-down list, choose **IP address** and enter the Cisco Cyber Vision Center IP address in the field to the right.
5. From the **Certificate Download Format** drop-down list, choose **PKCS12 format**.
6. Enter a certificate password in the two remaining fields, then click the **Create** button.

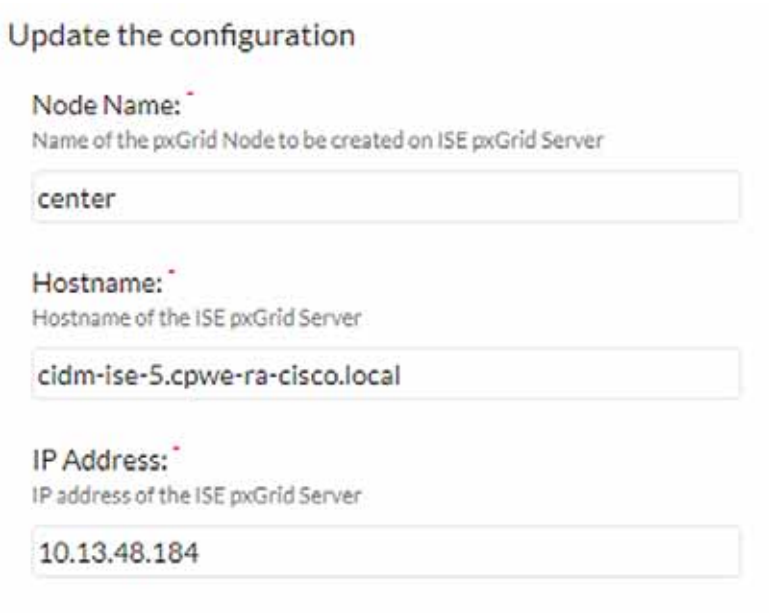
7. The certificate will automatically download to the user's system.

Configure the pxGrid Connection in Cisco Cyber Vision Center

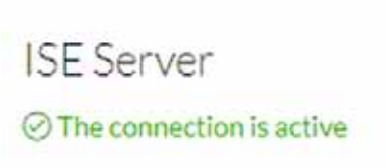
1. From the Cisco Cyber Vision Center web UI, choose **Admin** on the left menu pane.
2. Choose **PxGrid** from the **Admin** menu.
3. Under **Client Certificate**, click the **Change Certificate** button, and upload the certificate downloaded from ISE.

4. In the **Node Name** field, enter the common name used when generating the pxGrid certificate in ISE.
5. In the **Hostname** field, enter the fully-qualified domain name (FQDN) of the ISE pxGrid server.

6. In the **IP Address** field, enter the IP address of the ISE pxGrid server.



7. Click the **Update** button. A status message will be displayed on the page.



Integrating Cisco Cyber Vision Center with Cisco Stealthwatch

As with the ISE integration, Cisco Cyber Vision Center data can be used to augment Cisco Stealthwatch contextual information. Components in Cisco Cyber Vision Center can be grouped together, which can then be passed to Stealthwatch, forming or updating a Host Group; this integration associates asset IP addresses to intuitive group membership, which helps to accelerate attribution during network traffic analysis and threat investigation.

For more information on the Cisco Cyber Vision Center integration with Stealthwatch, see:

- https://www.cisco.com/c/dam/en/us/products/collateral/security/stealthwatch/at-a-glance-c45-736855.pdf.
- https://developer.cisco.com/stealthwatch/enterprise/

Cisco Cyber Vision Sensor Configuration

The Cisco Cyber Vision Sensor application performs deep packet inspection on network traffic to glean information about devices, software vulnerabilities, traffic protocols, and so on, particularly those of the industrial realm. Several hardware platforms and Cisco IOx software support the Cisco Cyber Vision Sensor application; the Cisco Catalyst 9300 and IE 3400 switches as well as the Industrial Compute 3000 (IC3000) gateway were validated with the Cisco Cyber Vision Sensor in this implementation.

Cisco Cyber Vision Sensor on the IC3000

Data Configuration

The Switched Port Analyzer (SPAN) feature in Cisco IOS sends data to the interface connected to the IC3000. The data from the source interface or VLAN is copied and sent to a destination interface, thus providing a full traffic stream for the IC3000 Cisco Cyber Vision Sensor deep packet inspection. To configure the SPAN on the switch, enter the following commands in enable mode:

```
Switch#conf t
Switch(config)#monitor session 1 source {vlan vlan_# | interface int_#}
Switch(config)#monitor session 1 destination interface interface_#
Switch(config)#end
```

Application Installation

Refer to the following for installing the Cisco Cyber Vision Sensor IOx application on the IC 3000:
https://www.cisco.com/c/en/us/td/docs/routers/ic3000/deployment/guide/DeploymentGuide-Cyber.html

Cisco Cyber Vision Sensor on the IE 3400

Data Configuration

The Encapsulated Remote Switched Port Analyzer (ERSPAN) feature in Cisco IOS sends data to the Cisco Cyber Vision Sensor application within the switch. ERSPAN creates copy of specified source traffic from a port or VLAN and sends it to an IP address, making use of generic routing encapsulation (GRE) allowing it to traverse to a remote destination across the Layer 3 network. The Cisco Cyber Vision Sensor interface that captures traffic is given an IP address in order to receive the data sent from the ERSPAN instance on the switch. To configure the ERSPAN on the switch, enter the following commands in enable mode:

```
Switch#conf t
Switch(config)#vlan destination_vlan_#
Switch(config-vlan)#remote-span
Switch(config-vlan)#exit
Switch(config)#monitor session 1 source {vlan vlan_# | interface int_#}
Switch(config)#monitor session 1 destination remote vlan destination_vlan_#
Switch(config)#monitor session 1 destination format-erspan IP_address
Switch(config)#end
```

IOx Configuration

The IE 3400 switch requires a 4GB SD card to be used for IOx applications. To format the SD card, enter the following command in enable mode:

```
Switch#format sdflash: ext4
```

To enable IOx, enter the following commands in enable mode:

```
Switch#conf t
Switch(config)#iox
Switch(config)#ip http server
Switch(config)#ip http secure-server
Switch(config)#end
```

Port Configuration

The Cisco Cyber Vision Sensor application communicates over IP to the Cisco Cyber Vision Center, therefore at least one interface (SVI or physical) must be configured with an IP address that is able to communicate through the network to the Cisco Cyber Vision Center. A VLAN interface was used in this implementation:

```
IE3400-3#sho run int vlan 15
```

```
!
interface Vlan15
 ip address 10.17.15.157 255.255.255.0
```

In addition, the AppGigabitEthernet interface must be configured as a trunk to transfer data to and from the Cisco Cyber Vision Sensor application:

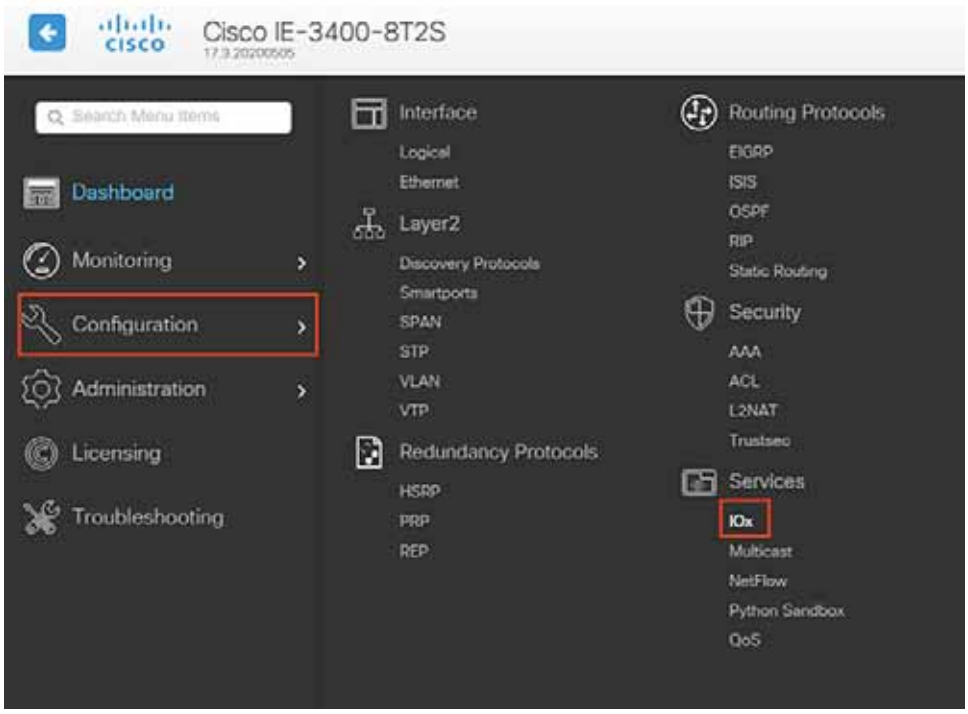
```
Switch#conf t
Switch(config)#interface AppGigabitEthernet 1/1
Switch(config)#switchport mode trunk
Switch(config)#end
```

Application Installation

The IE 3400 switch hosts the Cisco Cyber Vision Sensor in Cisco IOx and can be installed and managed from the CLI or the web GUI. This guide will cover the web GUI installation steps.

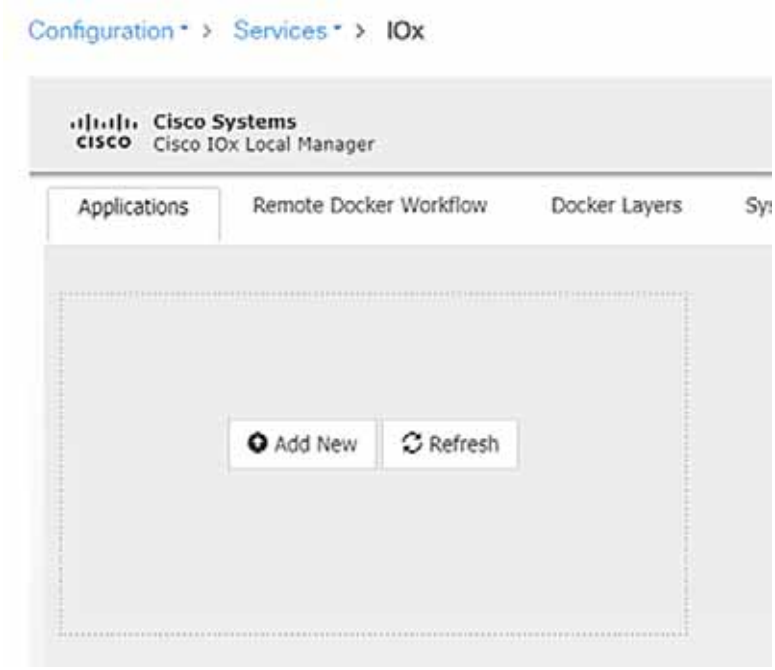
Note: IOS upgrades may affect the sensor application, requiring a reinstall.

1. In a web browser, navigate to the switch over HTTPS and log in with administrator credentials.
2. From the left menu, navigate to **Configuration -> Services -> IOx**.

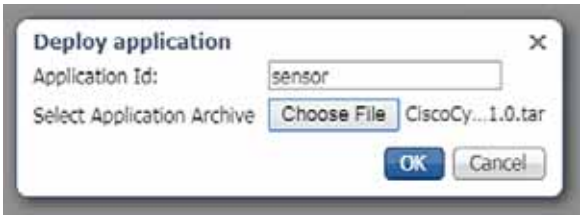


3. Log in to the Cisco IOx Local Manager with the same administrator credentials.

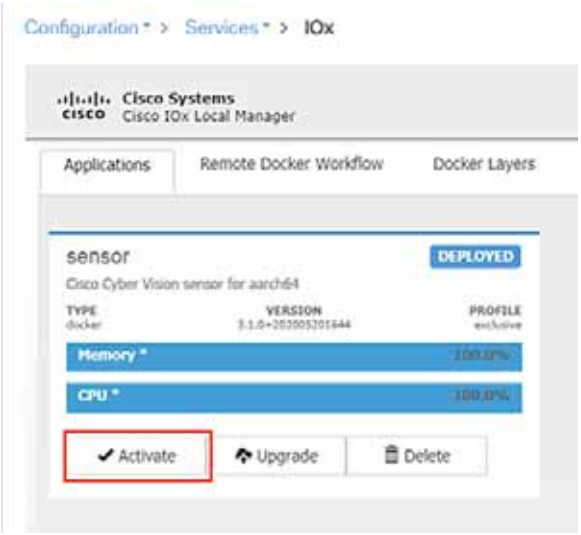
4. From the **Applications** tab, click the **Add New** button.



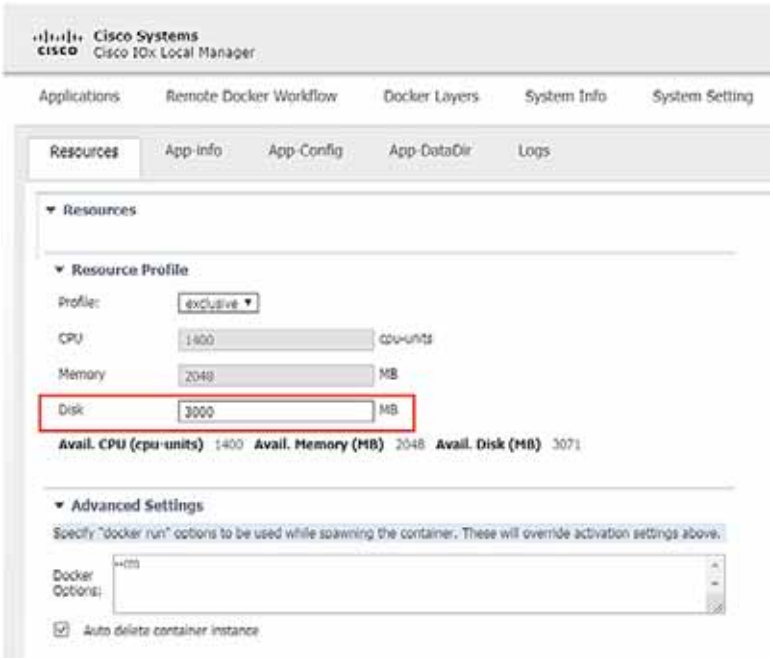
5. In the **Deploy application** dialog box, enter a name for the Cisco Cyber Vision Sensor application and click the **Browse** button to upload the .tar file for the IE 3400 Cisco Cyber Vision Sensor application. When finished, click the **OK** button.



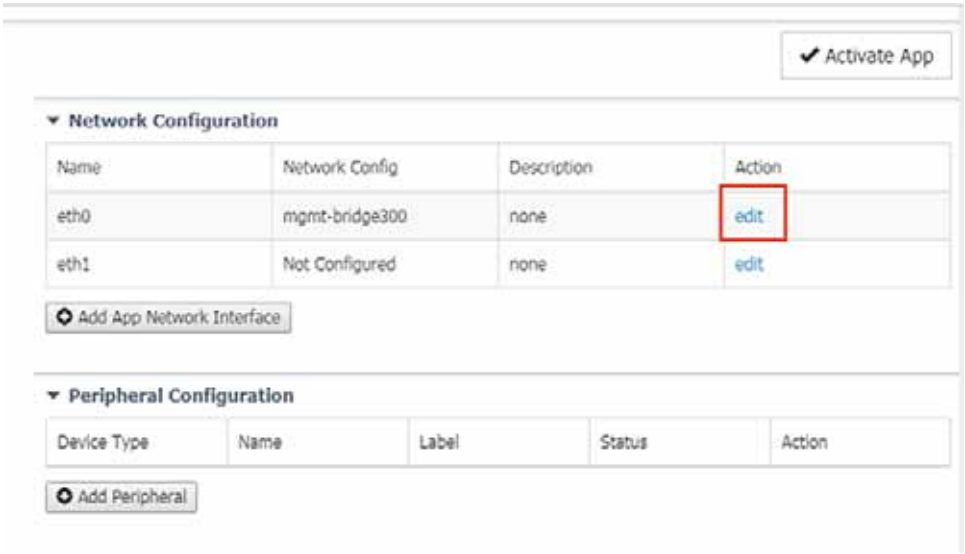
6. When the installation finishes, the application status will show as “DEPLOYED”. Click the **Activate** button.



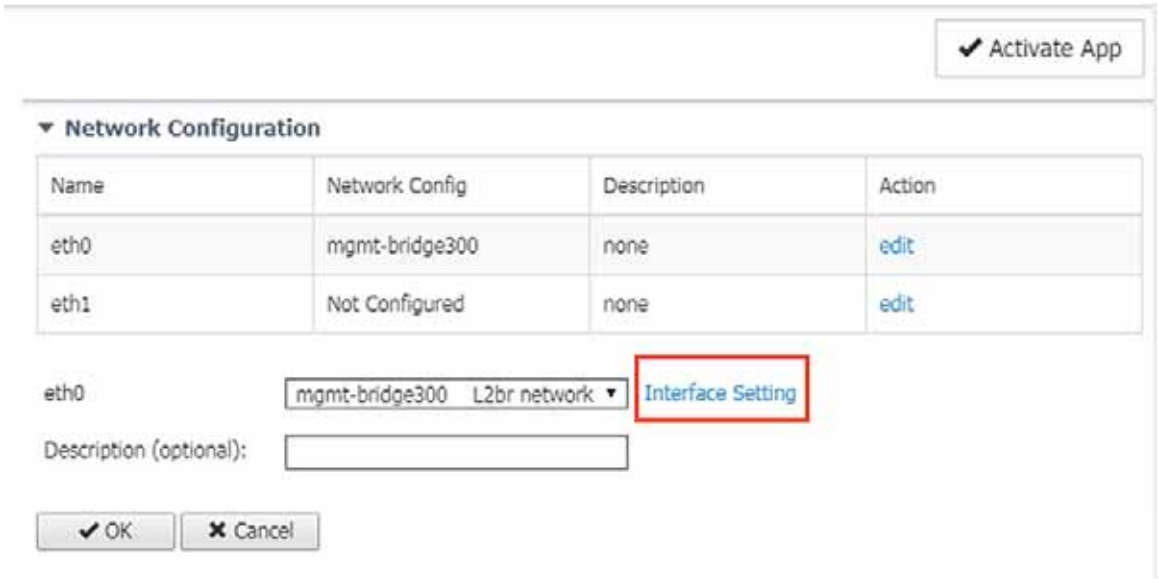
7. From the **Sensor -> Resources** tab, under **Resource Profile**, enter 3000 in the **Disk** field.



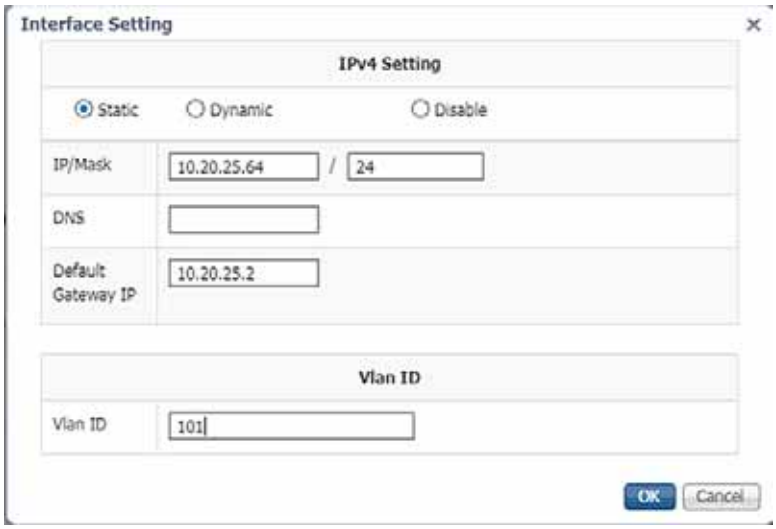
8. Under **Network Configuration**, click the **Edit** link for the eth0 interface.



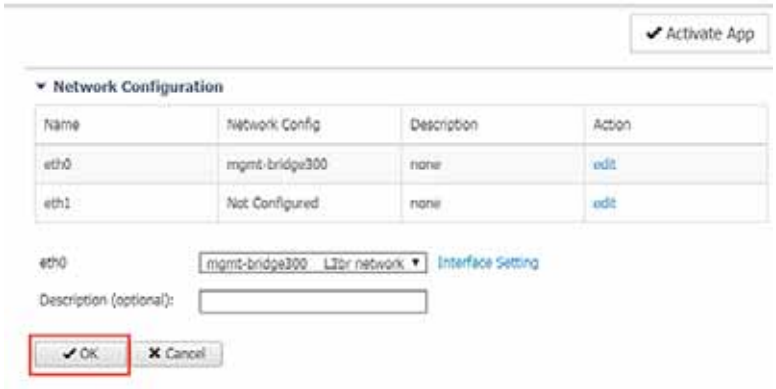
9. Click the **Interface Setting** link for eth0.

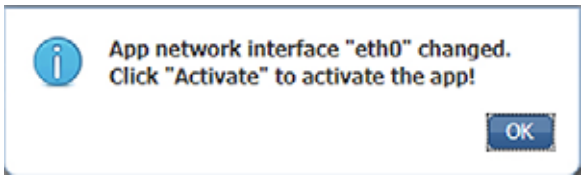


10. In the **Interface Setting** dialog box, click the **Static** radio button. Then enter values in the **IP**, **Mask**, **Default Gateway IP**, and **VLAN ID** fields. This information will be used for the Cisco Cyber Vision Sensor application communication to the Cisco Cyber Vision Center. When finished, click the **OK** button.

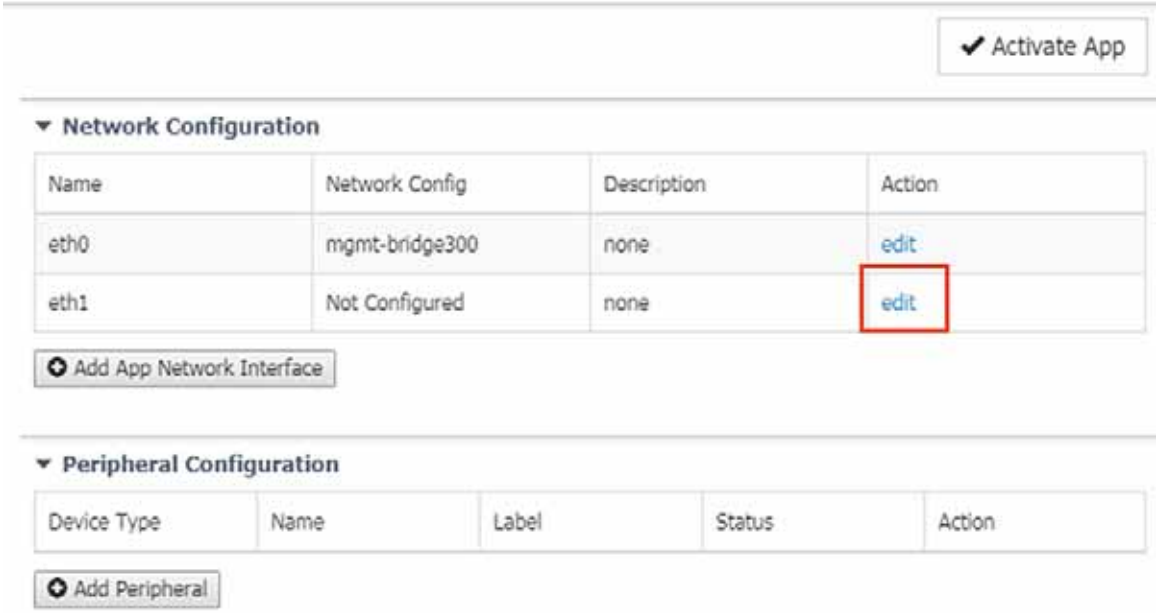


11. Click the **OK** button underneath the interface details, then click the **OK** button in the notification dialog box.

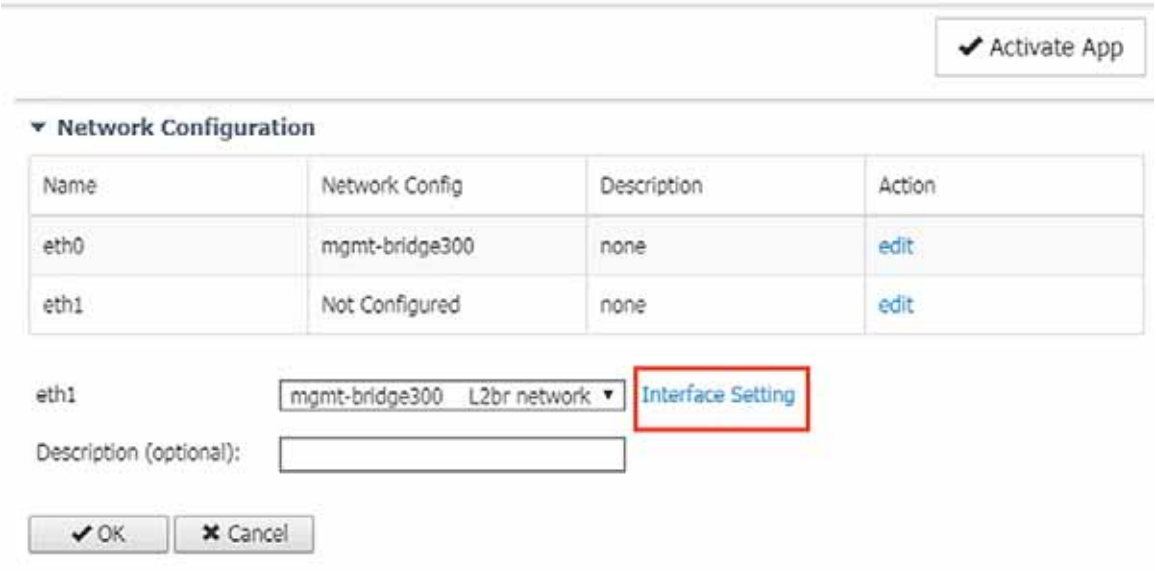




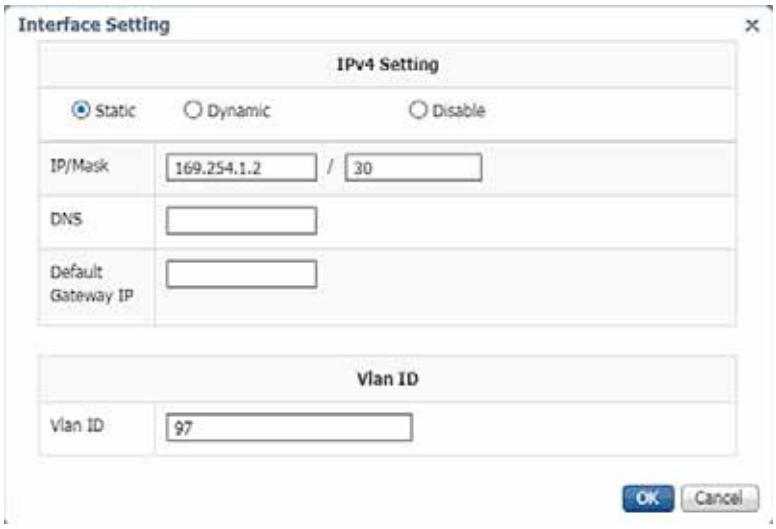
12. Under **Network Configuration**, click the **Edit** link for the eth1 interface.



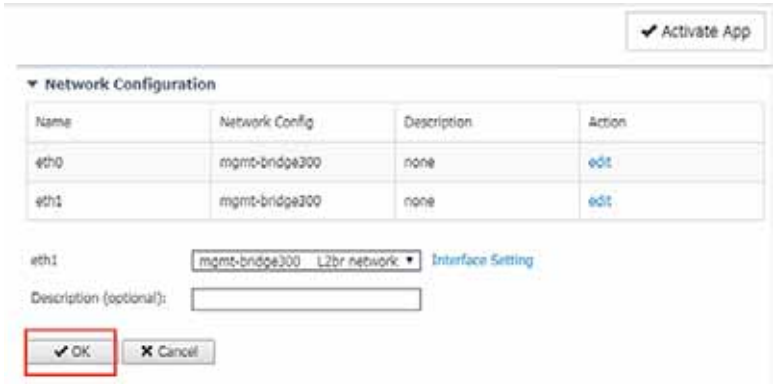
13. Click the **Interface Setting** link for eth1.

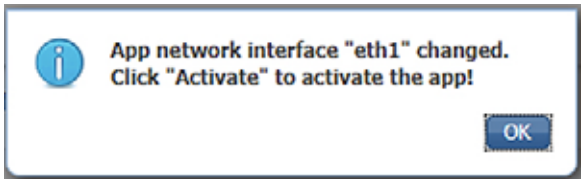


14. In the **Interface Setting** dialog box, click the **Static** radio button. Then enter values in the **IP**, **Mask**, and **VLAN ID** fields. This information should align with the ERSPAN destination configured on the switch. When finished, click the **OK** button.

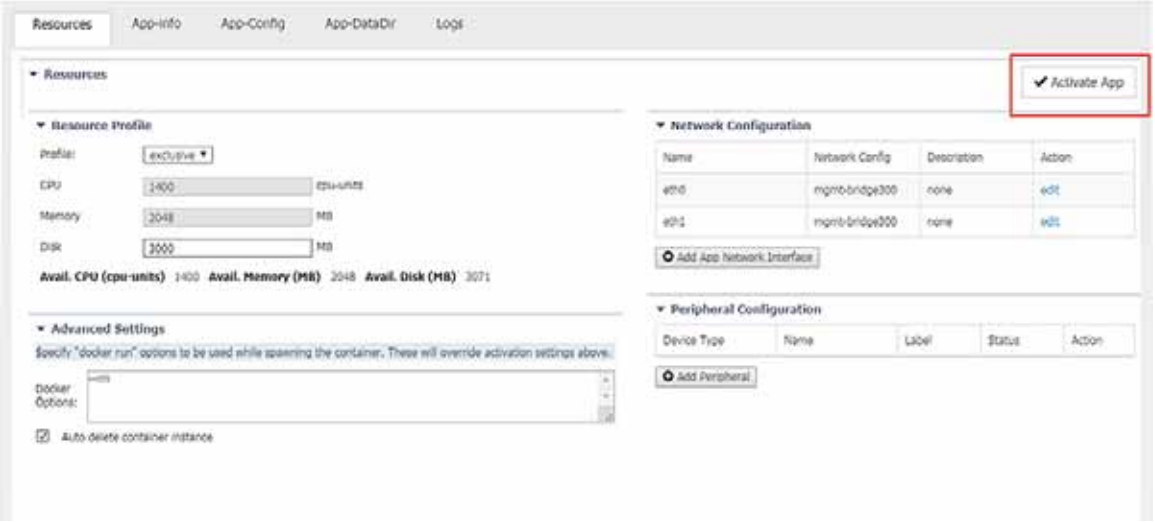


15. Click the **OK** button underneath the interface details, then click the **OK** button in the notification dialog box.

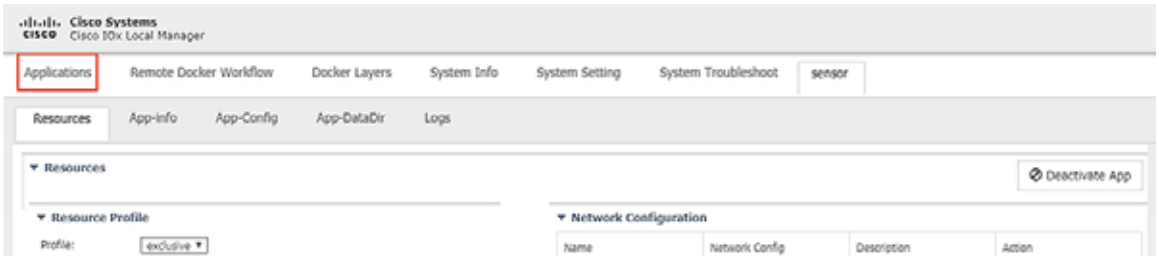




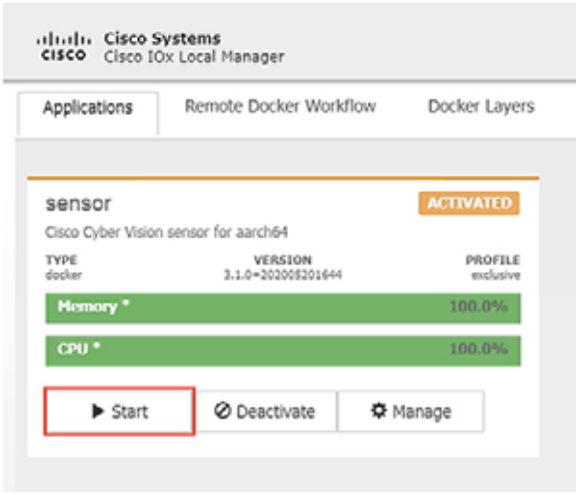
16. Click the **Activate App** button at the top right of the **Resources** tab page.



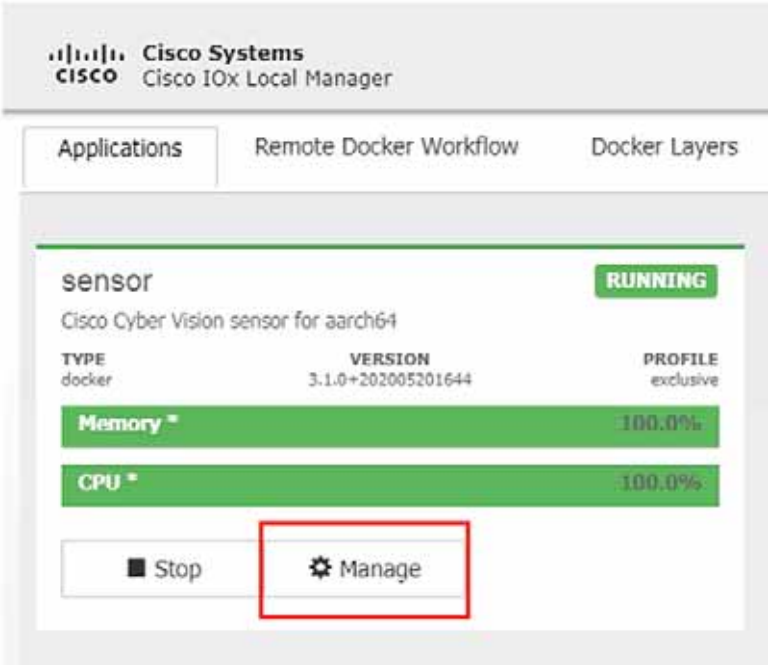
17. Once it is activated, click the **Applications** tab.



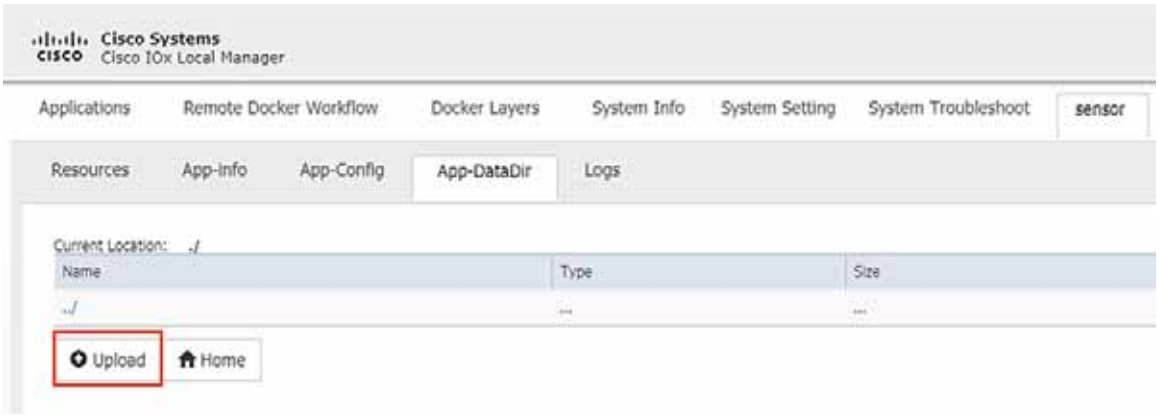
18. The application status will now show as “Activated”. Click the **Start** button.



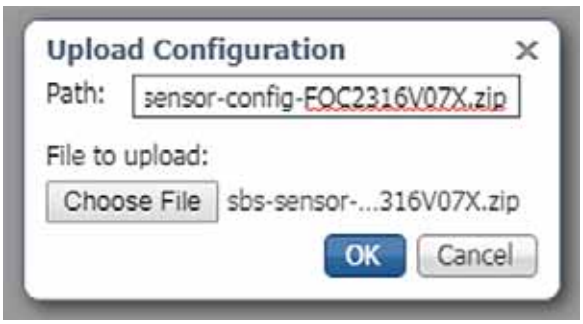
19. After it starts, the application status will show as “Running”. Click the **Manage** button.



20. Navigate to the **Sensor -> App-DataDir** tab. Click the **Upload** button.



21. Click the **Choose File** button to upload the provisioning package for the sensor specific to this switch (see Cisco Cyber Vision Center Configuration). In the **Path** field, enter the filename of the provisioning package, including the .zip extension. When finished, click the **OK** button.



22. Click the **OK** button in the notification dialog box.

Cisco Cyber Vision Sensor on the Cisco Catalyst 9300

Data Configuration

As with the IE 3400 switch, the Cisco Catalyst 9300 switch uses ERSPAN to copy traffic to the Cisco Cyber Vision Sensor application. To configure the ERSPAN on the switch, enter the following commands in enable mode:

```
Switch#conf t
Switch(config)#monitor session 1 type erspan-source
Switch(config-mon-erspan-src)#source {interface int_#_or list | vlan vlan_#_or_list}
Switch(config-mon-erspan-src)#destination
Switch(config-mon-erspan-src-dst)#erspan-id 2
Switch(config-mon-erspan-src-dst)#mtu 9000
Switch(config-mon-erspan-src-dst)#ip address IP_address
Switch(config-mon-erspan-src-dst)#origin ip address IP_address
Switch(config-mon-erspan-src-dst)#end
```

IOx Configuration

The Cisco Catalyst 9300 switch requires a Solid State Drive (SSD) for IOx applications. For more information about installing the SSD, see: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/hardware/install/b_c9300_hig/b_c9300_hig_chapter_01010.html.

If the Cisco Catalyst 9300 is in a StackWise-480 configuration, the switch with the SSD must be in the “active” role. To format the SSD, enter the following command in enable mode:

```
Switch#format usbflash1: ext4
```

To enable IOx, enter the following commands in enable mode:

```
Switch#conf t
Switch(config)#iox
Switch(config)#ip http server
Switch(config)#ip http secure-server
Switch(config)#end
```

Port Configuration

The Cisco Cyber Vision Sensor application communicates over IP to the Cisco Cyber Vision Center, therefore at least one interface (SVI or physical) must be configured with an IP address that is able to communicate through the network to the Cisco Cyber Vision Center. A VLAN interface was used in this implementation:

```
Cat9300#sho run int vlan 15
!
interface Vlan15
 ip address 10.17.15.1 255.255.255.0
```

Application Installation

The Cisco Catalyst 9300 switch hosts the Cisco Cyber Vision Sensor in Cisco IOx and can be installed and managed from the CLI or the web GUI. This guide will cover the CLI installation steps.

1. Configure the application name.

```
Cat9300(config)#app-hosting appid sensor_name
```

2. Configure the AppGigabitEthernet interface as a trunk.

```
Cat9300(config-app-hosting)#app-vnic AppGigabitEthernet trunk
```

3. Configure the Cisco Cyber Vision Sensor management interface.

```
Cat9300(config-config-app-hosting-trunk)#vlan vlan_# guest-interface 0
Cat9300(config-config-app-hosting-vlan-access-ip)#guest-ipaddress IP_address netmask
netmask_#.#.#.#
```

4. Configure the Cisco Cyber Vision Sensor capture interface.

```
Cat9300(config-config-app-hosting-trunk)#vlan vlan_# guest-interface 1
Cat9300(config-config-app-hosting-vlan-access-ip)#guest-ipaddress IP_address netmask
netmask_#.#.#.#
```

5. Configure gateway for the Cisco Cyber Vision Sensor management interface to use.

```
Cat9300(config-app-hosting)#app-default-gateway gateway_IP guest-interface 0
```

6. Configure gateway for the Cisco Cyber Vision Sensor application resources.

```
Cat9300(config-app-hosting)#app-resource profile custom
Cat9300(config-app-resource-profile-custom)#persist-disk 3000
Cat9300(config-app-resource-profile-custom)#cpu 7400
Cat9300(config-app-resource-profile-custom)#memory 2048
Cat9300(config-app-resource-profile-custom)#vcpu 2
Cat9300(config-app-resource-profile-custom)#end
```

7. Copy the .tar file for the Cisco Catalyst 9300 Cisco Cyber Vision Sensor to the SSD. Next, install the application.

```
Cat9300#app-hosting install app-id sensor_name package
usbflash1:CiscoCyberVision-IOx-x86-64-3.1.0.tar
```

8. Activate the application.

```
Cat9300#app-hosting activate app-id sensor_name
```

9. Start the application.

```
Cat9300#app-hosting start app-id sensor_name
```

10. Copy the provisioning package for the sensor specific to this switch to the application (see Cisco Cyber Vision Center Configuration).

```
Cat9300# app-hosting data appid sensor_name copy usbflash1:9300package.zip 9300package.zip
```

Cisco Stealthwatch Configuration

Installation

For this implementation, the SMC was deployed as a VM in the Enterprise Zone, and the FCs were deployed as VMs in the Level 3 Site Operations Zone. For VM installation instructions refer to: https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system_installation_configuration/SW_7_2_Installation_and_Configuration_Guide_DV_2_0.pdf.

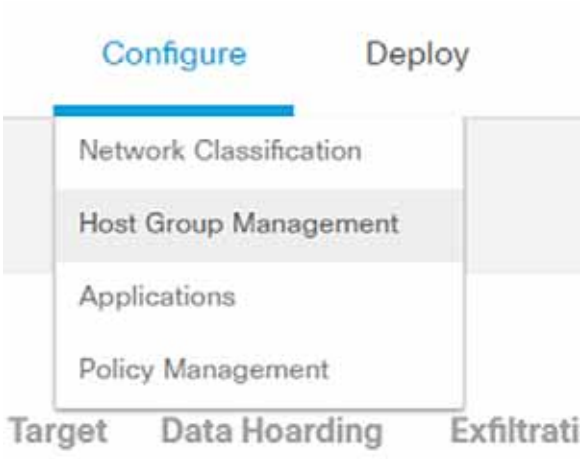
Java Client and Web UI

The SMC can be accessed two ways: Java client and web UI. Many of the features and functions of the traditional Java client have been ported to the web UI, however, some features are not yet available on the web UI (for example, Response Management). Alternatively, there are newer features only available to the web UI (for example, Custom Security Events). In this guide we have prioritized web UI configuration where possible.

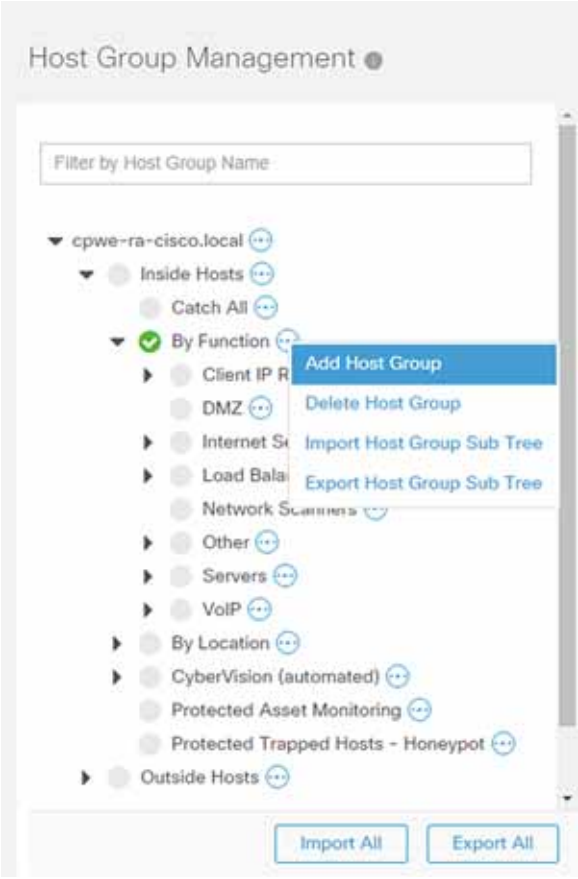
Host Groups

Stealthwatch Host Groups allow the user to organize IP addresses into intuitive groupings for ease of searching, alarm tuning, and host attribution. The preferred method of arranging addresses is to group by function; by grouping like devices that have similar behaviors, alarms and security events can be more easily refined for those entities. To create a Host Group in the SMC web UI, do the following:

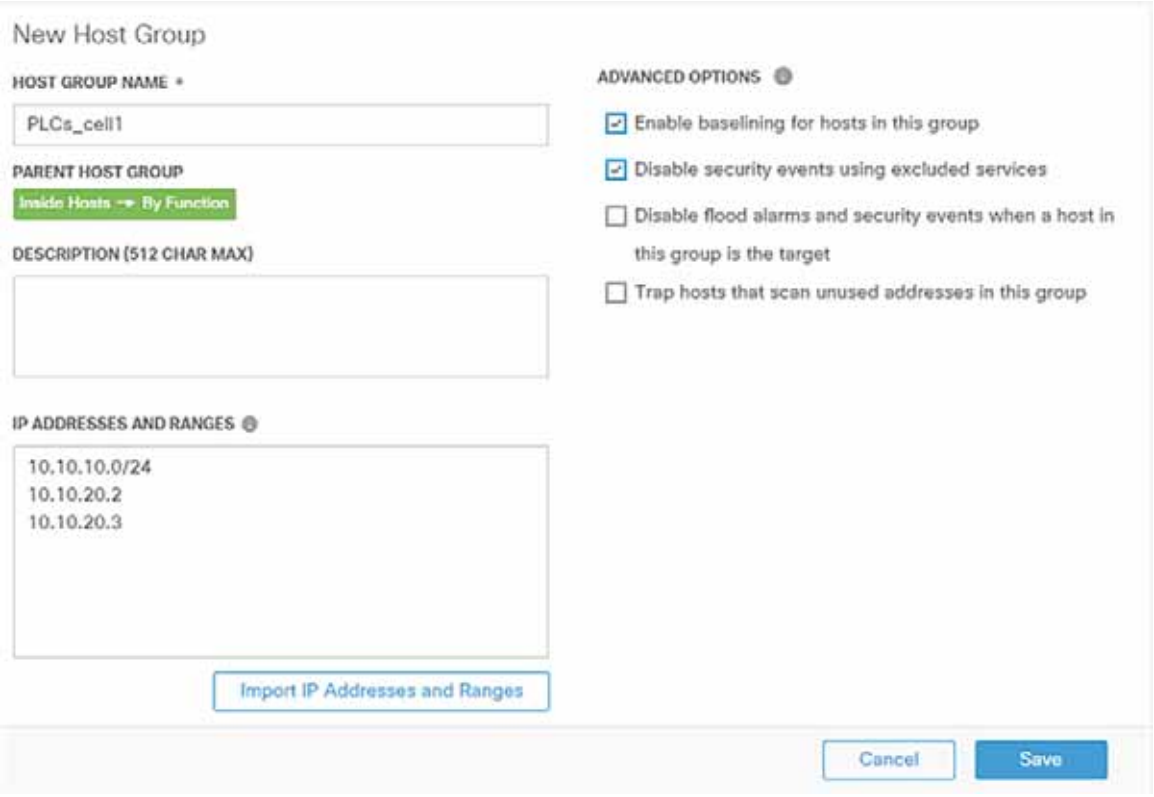
1. Navigate to **Configure -> Host Group Management**.



2. Click the **ellipses** button to the right of the Host Group for which you would like to create a nested Host Group. Choose **Add Host Group** from the list.



3. Enter information in the **Host Group Name** and **IP Addresses and Ranges** fields. Check the **Advanced Options** check boxes as needed.

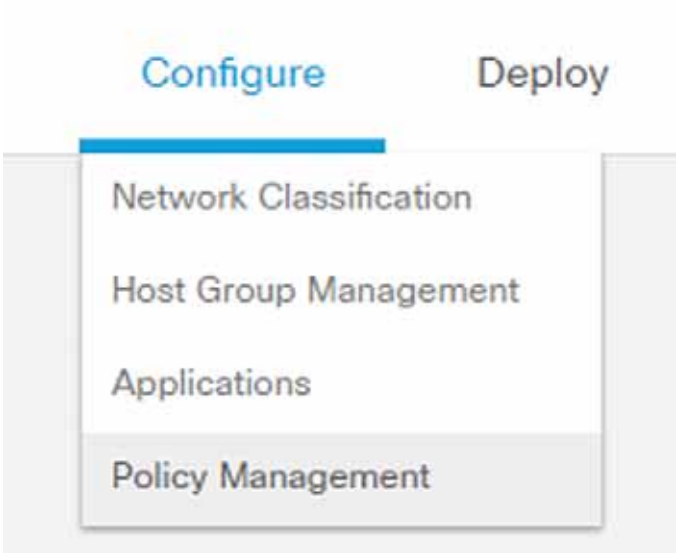


4. Click the **Save** button.

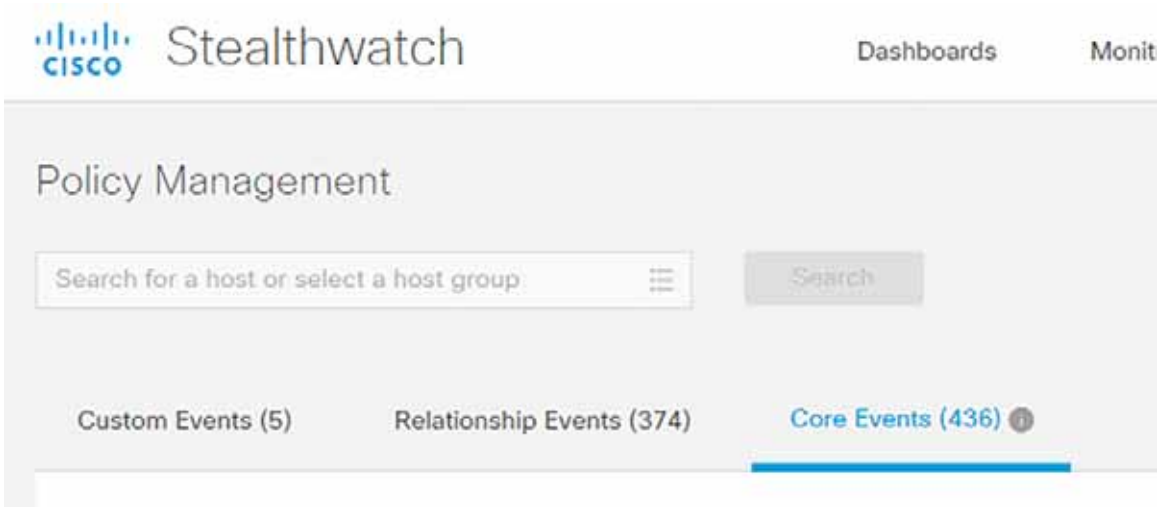
Host Policy

Host Policy allows the user to tailor the security events and alarm categories applied for a particular host or Host Group. Most security events have a configurable threshold to meet specific requirements for a given entity. To create or edit a Host Policy in the SMC web UI, do the following:

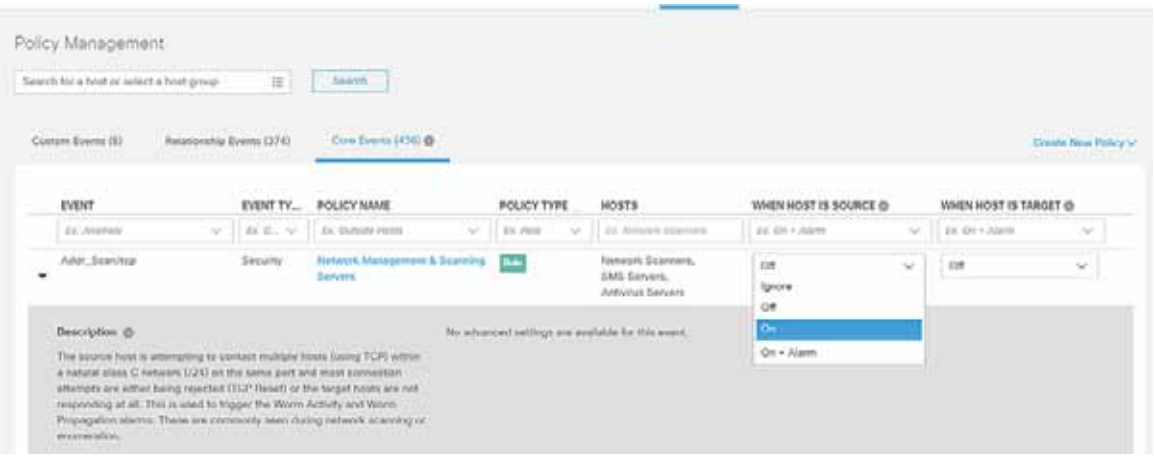
1. Navigate to **Configure > Policy Management**.



2. Click the **Core Events** link to view current global security events and their settings.

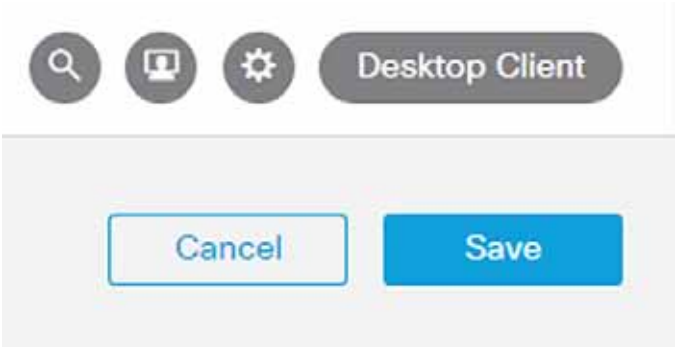


3. Turn global security events or categories on or off using the **When Host is Source** and **When Host is Target** drop-down lists.



4. Update the thresholds for necessary events or categories by clicking the **Behavioral and Threshold** or **Threshold Only** radio button.

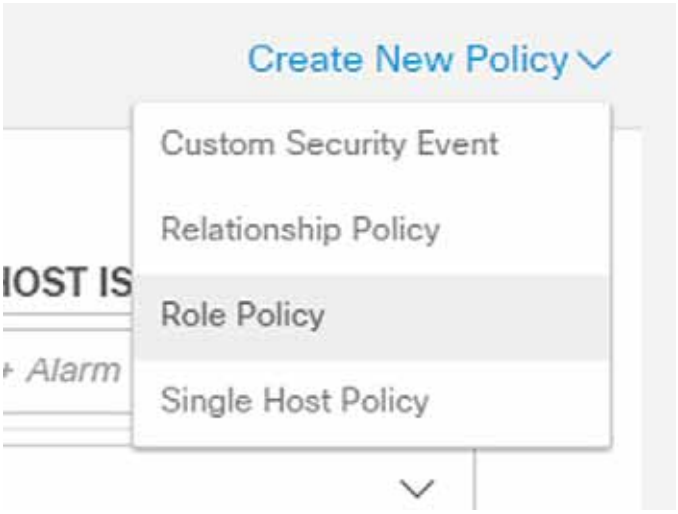
5. Click the **Save** button.



To create a custom policy for IP address(es), Host Group(s), or both, do the following:

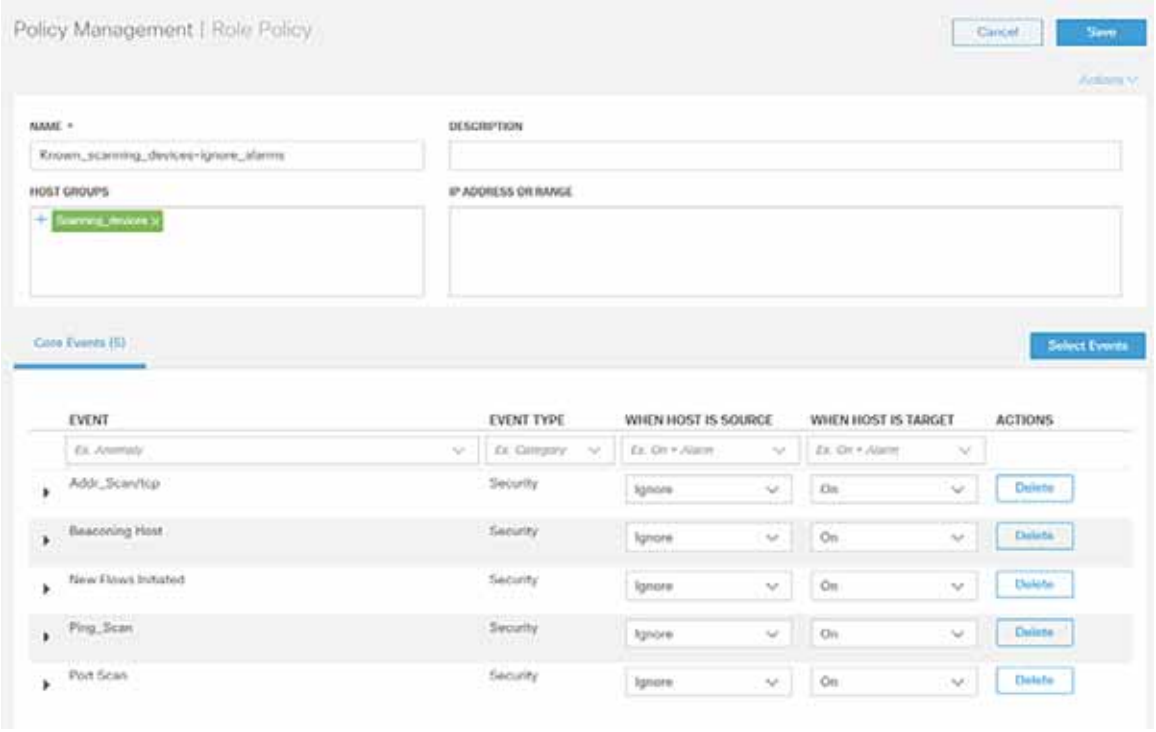
1. Navigate to **Configure -> Policy Management**.

2. From the **Create New Policy** drop-down list, choose **Role Policy**.



3. Enter a name for the policy and add Host Groups, IP address(es), or both.

4. Click the **Select Events** button to add events. Use the **When Host is Source** and **When Host is Target** drop-down lists to enable or disable the events for the specified entities.

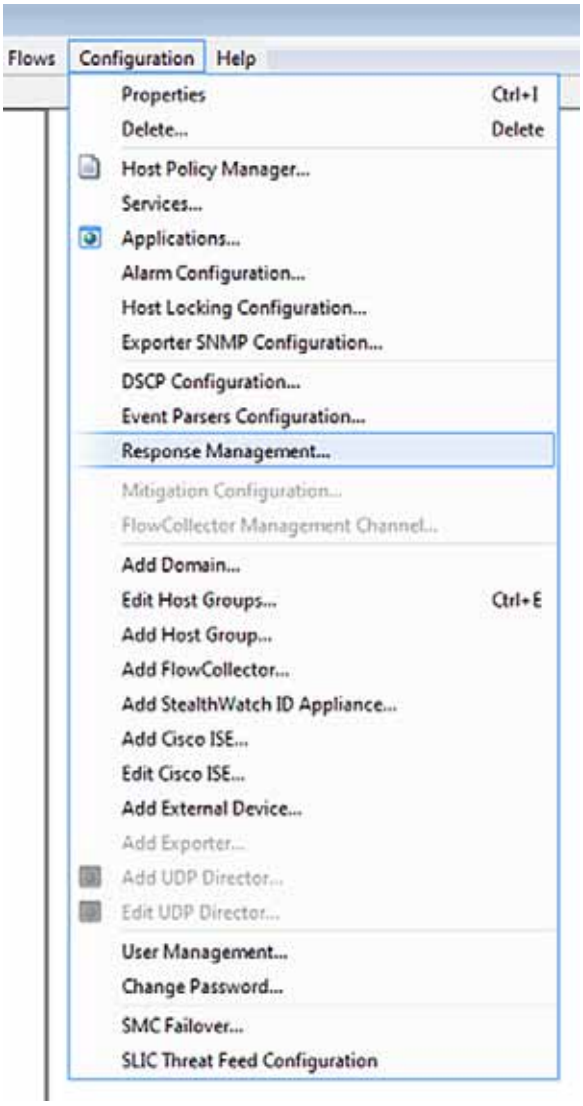


5. Click the **Save** button.

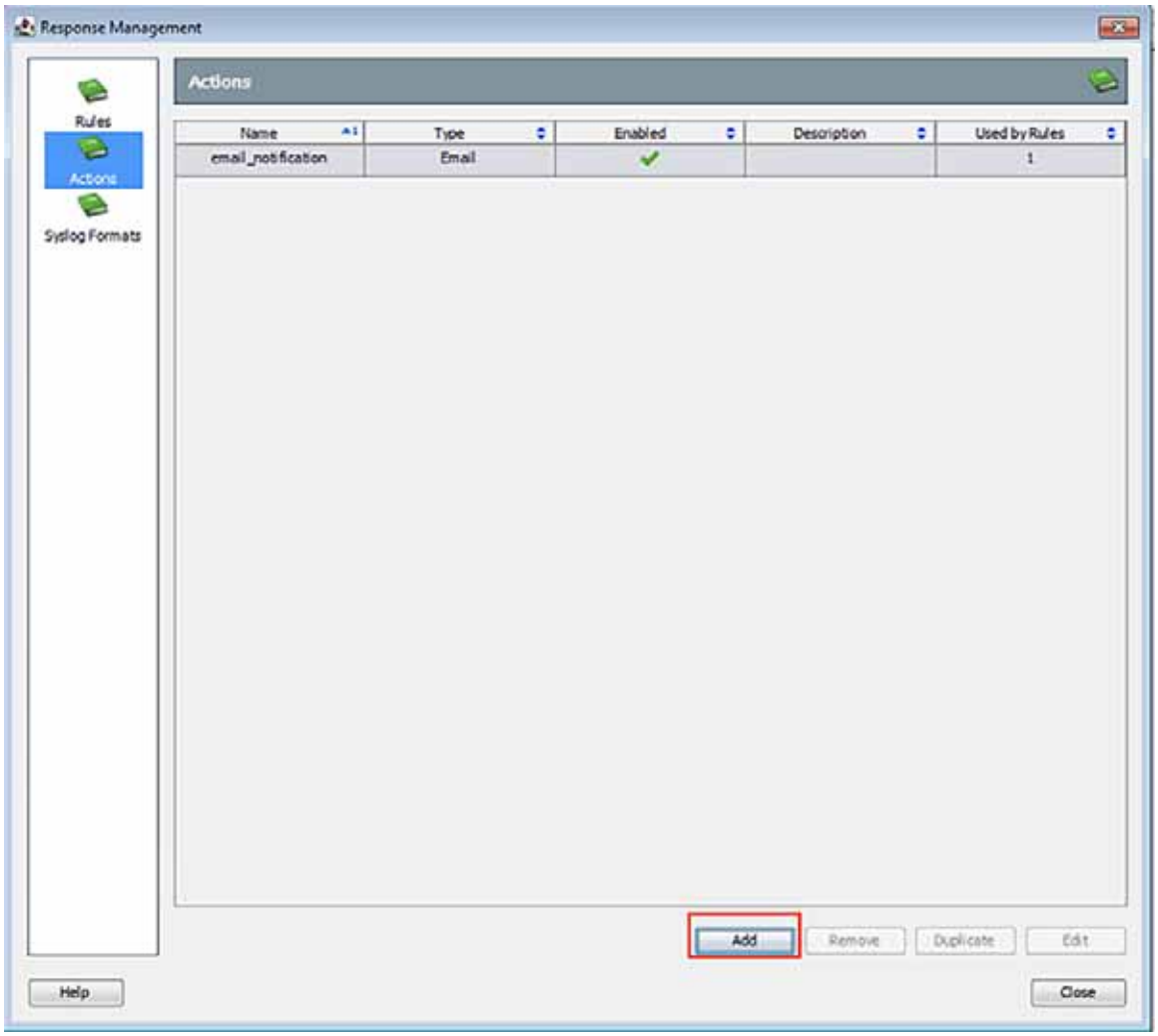
Alarm Notifications

Alarms can be viewed in the SMC, but also sent from the SMC as email notifications or syslog messages. To configure alarm notifications from the SMC Java UI, do the following:

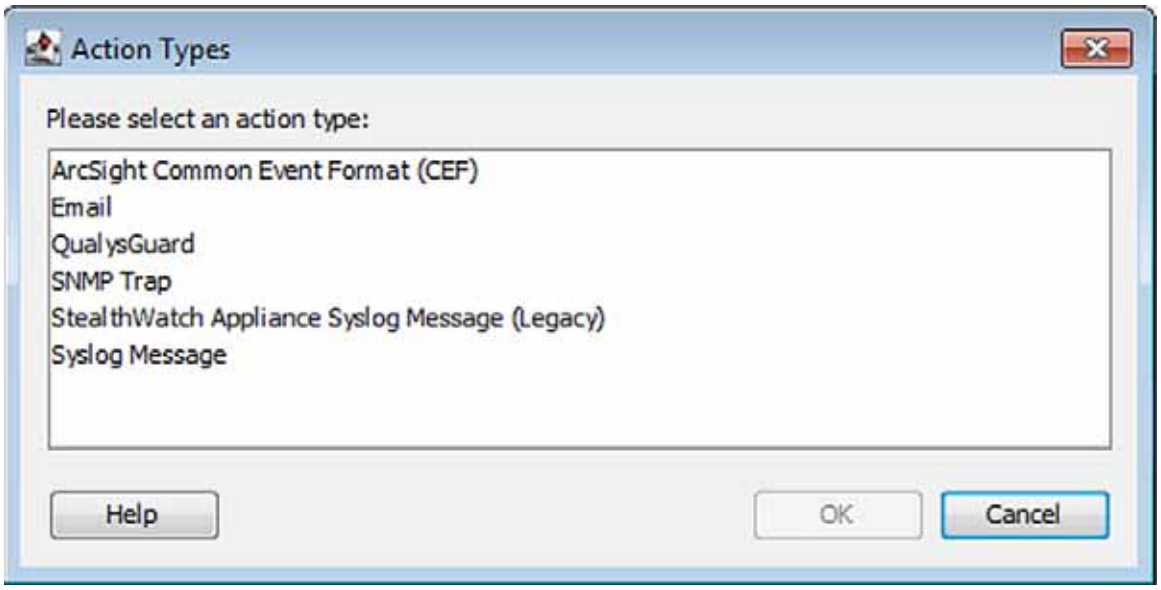
1. Navigate to **Configuration -> Response Management**.



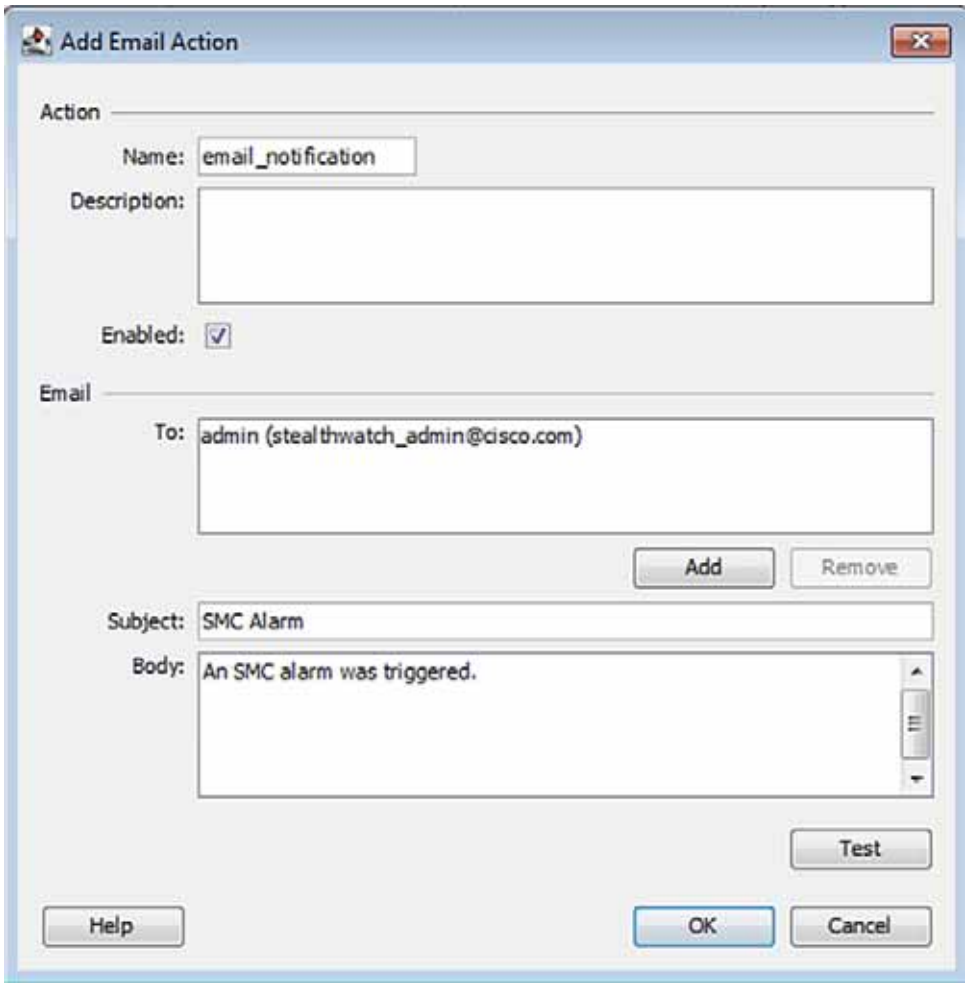
2. From the **Response Management** window **Actions** pane, click the **Add** button.



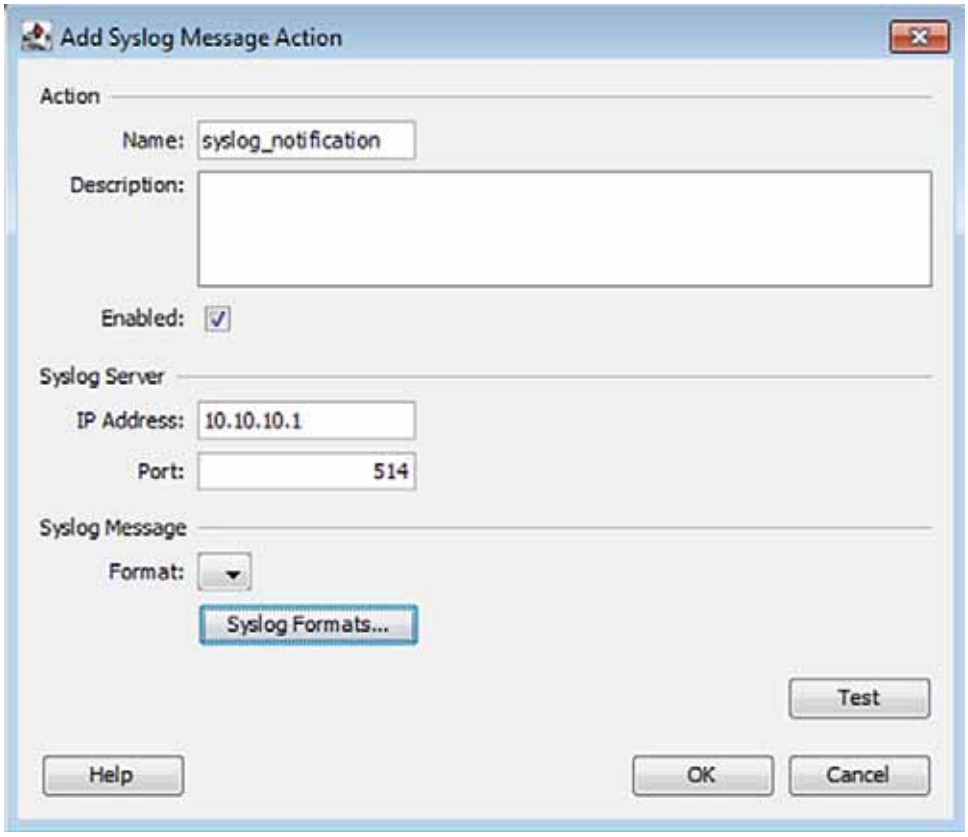
3. In the **Action Types** dialog box, choose the appropriate action.



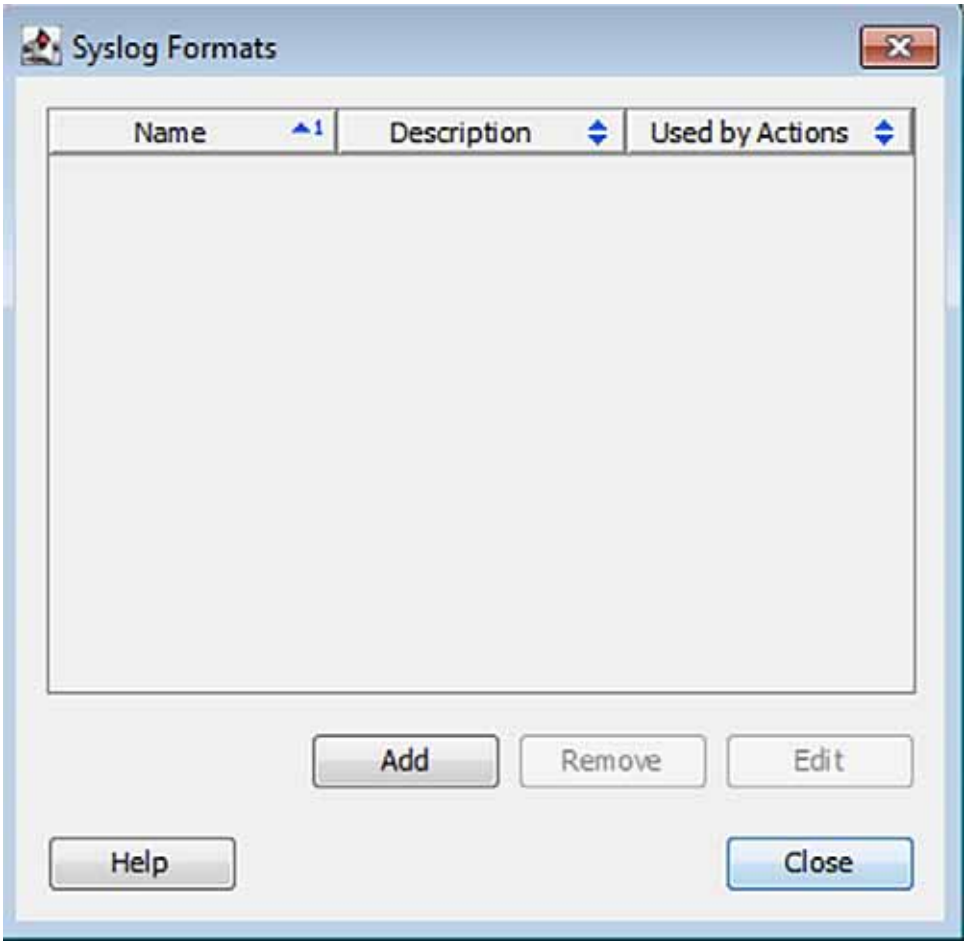
4. If choosing the **Email** action type, in the **Add Email Action** window enter the action name, recipient, email subject, and email body. Click the **OK** button when finished.



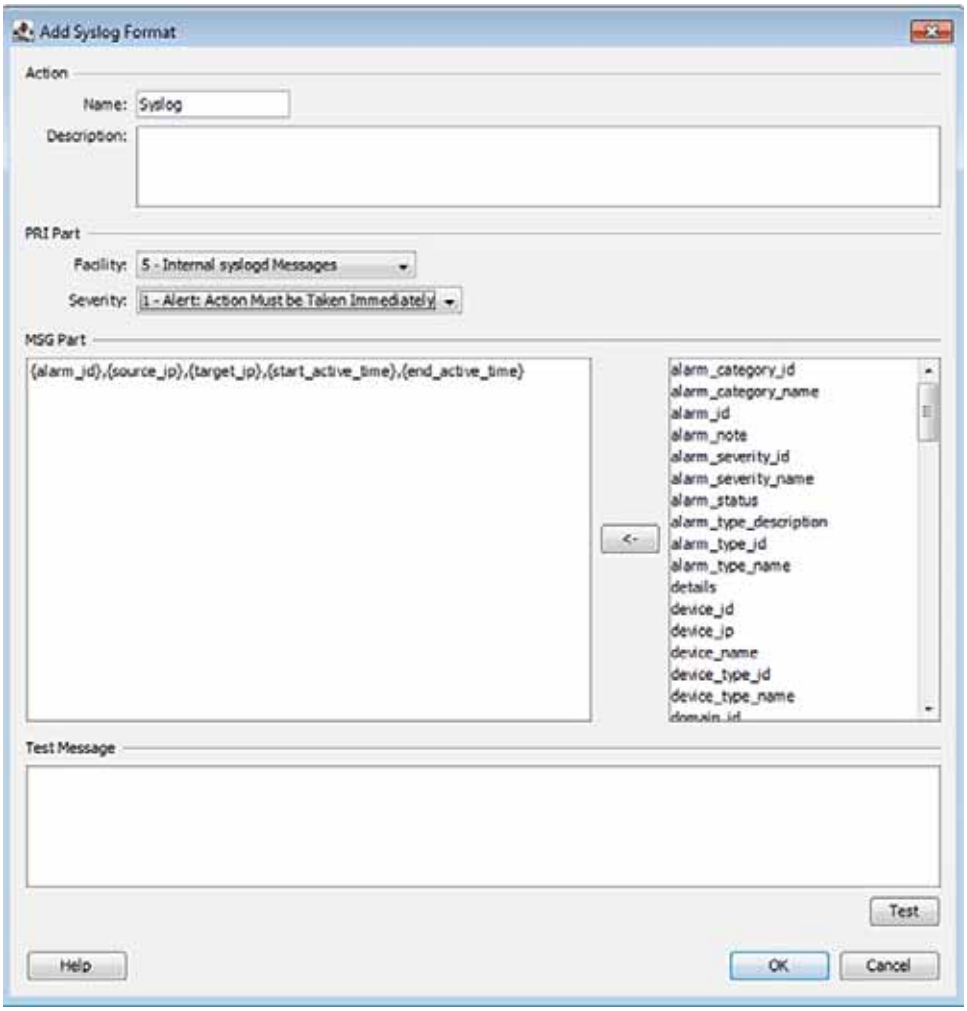
5. If choosing the **Syslog Message** action type, in the **Add Syslog Message Action** window enter the action name, syslog server IP address, and syslog server port. Click the **Syslog Formats** button to create a Syslog Format if none have been previously configured. Otherwise, choose a format from the **Format** drop-down list and click the **OK** button.



6. If no syslog format has been created and you have clicked the **Syslog Formats** button, in the **Syslog Formats** window, click the **Add** button.

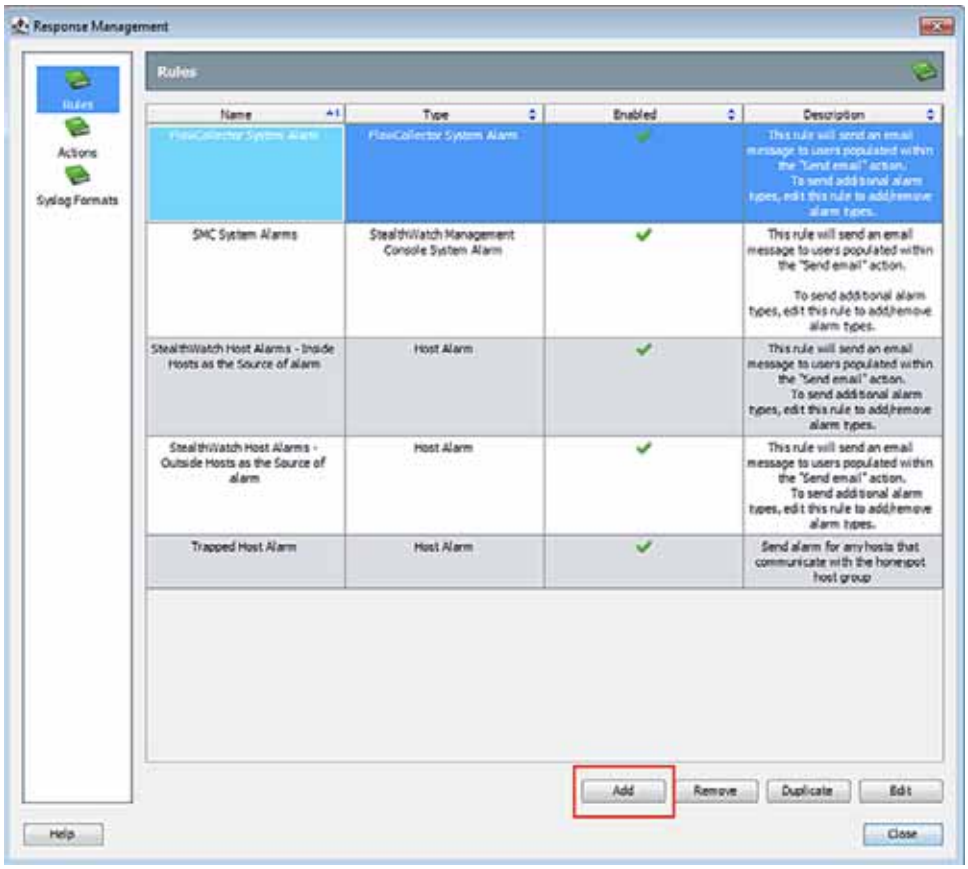


7. In the **Add Syslog Format** window, enter a name, choose the facility and severity, and update the message content as desired.



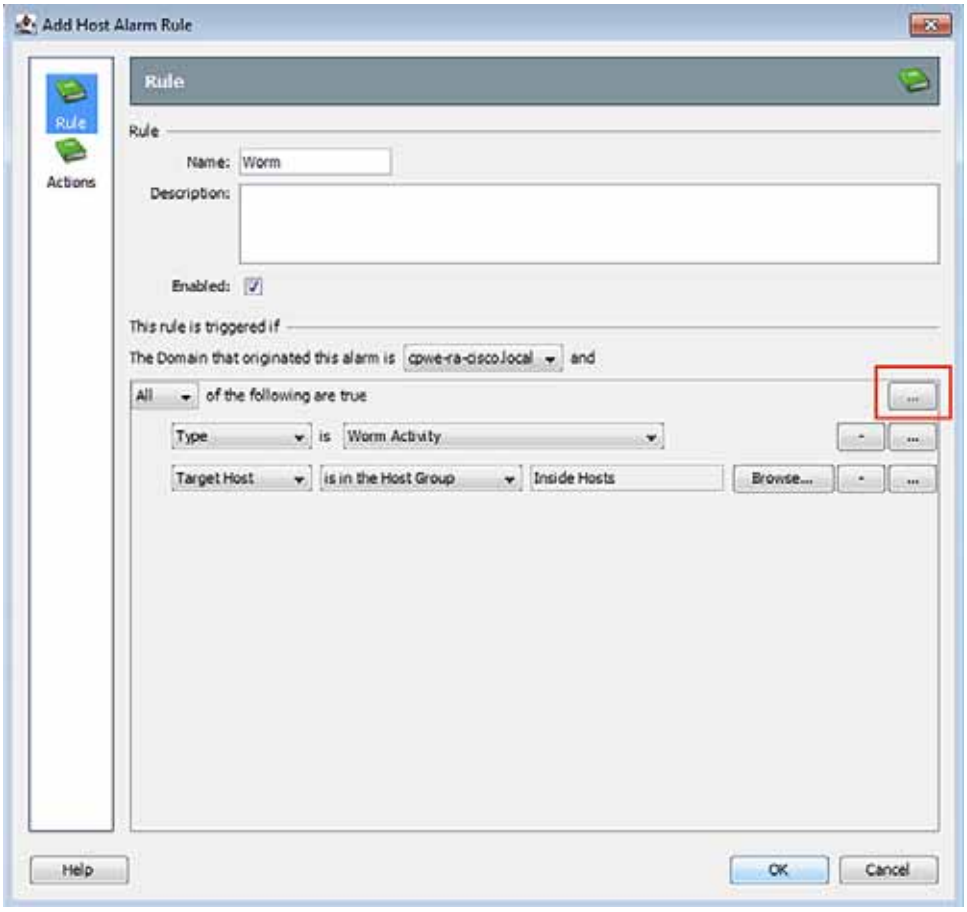
Click the **OK** button when finished.

8. From the **Response Management** window **Rules** pane, click the **Add** button.

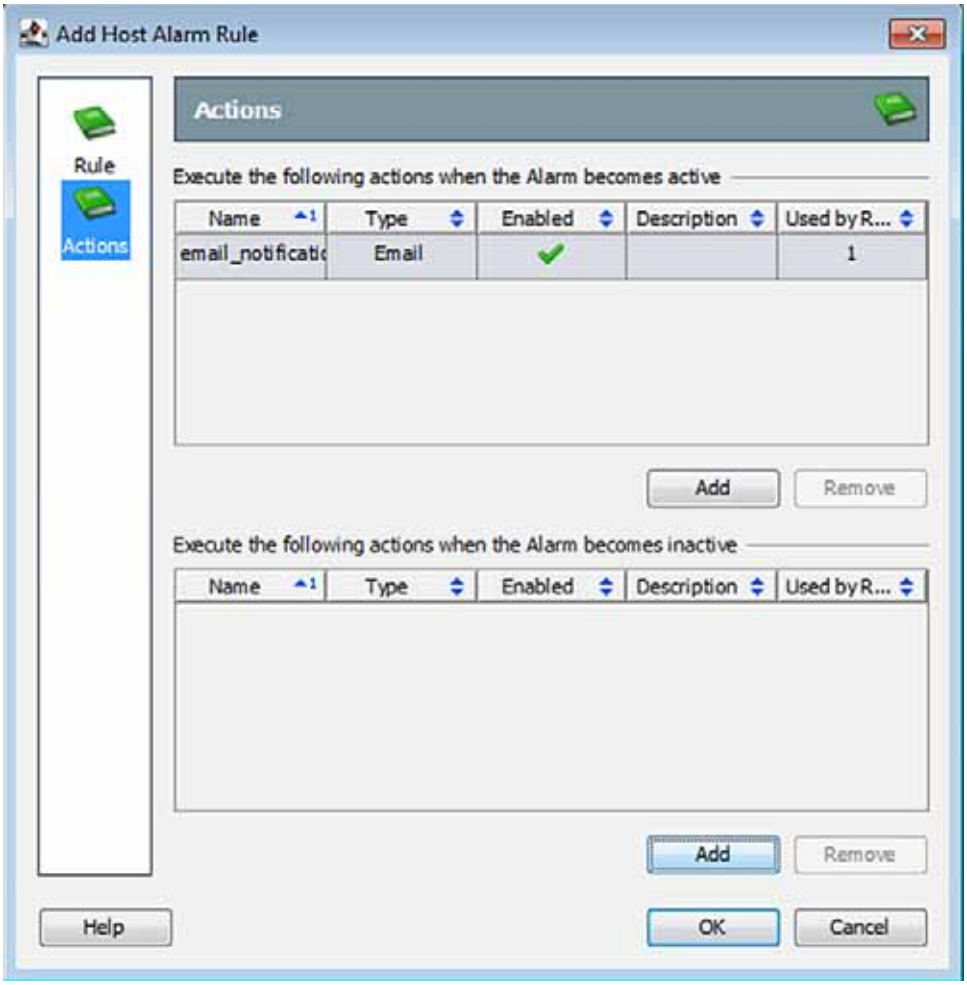


9. Choose **Host Alarm** from the **Rule Types** dialog box.

10. In the **Add Host Alarm Rule** window, in the **Rule** pane enter a name and the use the **ellipses** button to add alarm conditions.



11. In the **Actions** pane, click the **Add** buttons to update the actions for the active and inactive Alarm states. Click the **OK** button when finished.



Precision Time Protocol Configuration

This section describes the implementation of site-wide Precision Time Protocol (PTP) for Industrial Automation environments.

There are three deployment options based on customer precision requirements:

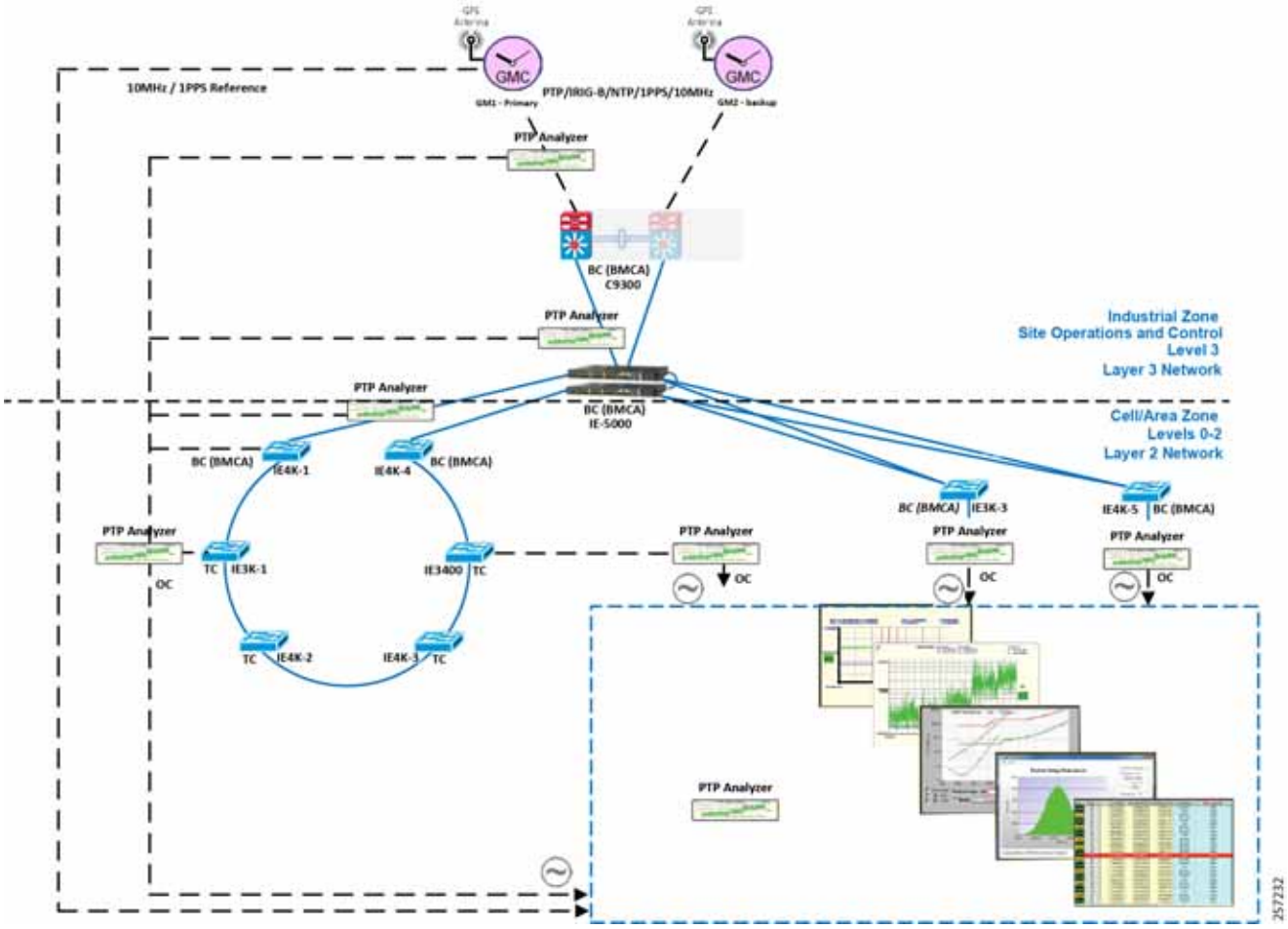
- High Precision site-wide time distribution using a dedicated grandmaster clock

  The plantwide high precision grandmaster clock time distribution architecture provides a plantwide, highly accurate time feed forward tree to facilitate inter-cell loop or plantwide motion drive cooperation. It normally requires high accuracy oscillators to synchronize with a GNSS source.

  Grandmaster clock source redundancy, transport network device box-level redundancy (for example stack-wise, HSRP over industrial zone), Cell/Area Zone resilient network topology, etc., all provide redundant PTP message source and transport path. This highly resilient network design reduces the possibility that any network element will lose its clock source. If, in a very extreme case, the clock source become unavailable, a multi-level boundary clock will enter into a “HOLDOVER” state to assume the primary clock role for its lower stratum clock element to maintain normal industrial operations.

Figure 42 shows the plantwide high precision grandmaster clock architecture.

Figure 42 Plantwide High Precision GPS Backed PTPv2 Architecture



Where:

- Meinberg LANTIME M600 provides redundant plant-wide grandmaster clocks.
- Cisco Catalyst 9300 core switch is configured as Boundary Clock (BC) over industrial zone.
- Cisco IE 5000 pair switches are configured as BC over distribution layer.
- Cisco IE 4000 pair switches are configured as BC on the top of each ring or start to dual-home to distribution switch pairs.
- Cisco IE 4000 is configured as end-to-end Transparent Clock (TC) inside ring.
- Cisco IE 3000 is configured as end-to-end TC inside ring.
- Cisco IE 3400 is configured as end-to-end TC inside ring.
- Customer PLC controller IP module is configured as Ordinary Clock (OC) to recover clock.
- Underlying resilience protocols vary with MSTP, REP, etc. deployed transport protocols.
- Industrial Ethernet Switch is enabled with PTP-aware QoS for classifying and policing PTP messages.

Note: The Cisco Catalyst 9300 will support PTPv2 over VSS stacking in the future. Cisco IE 5000 stack-wise does not currently support PTP. In the topology in Figure 42, Cisco IE 5000 pairs are configured with HSRP over a Layer 2 trunk link.

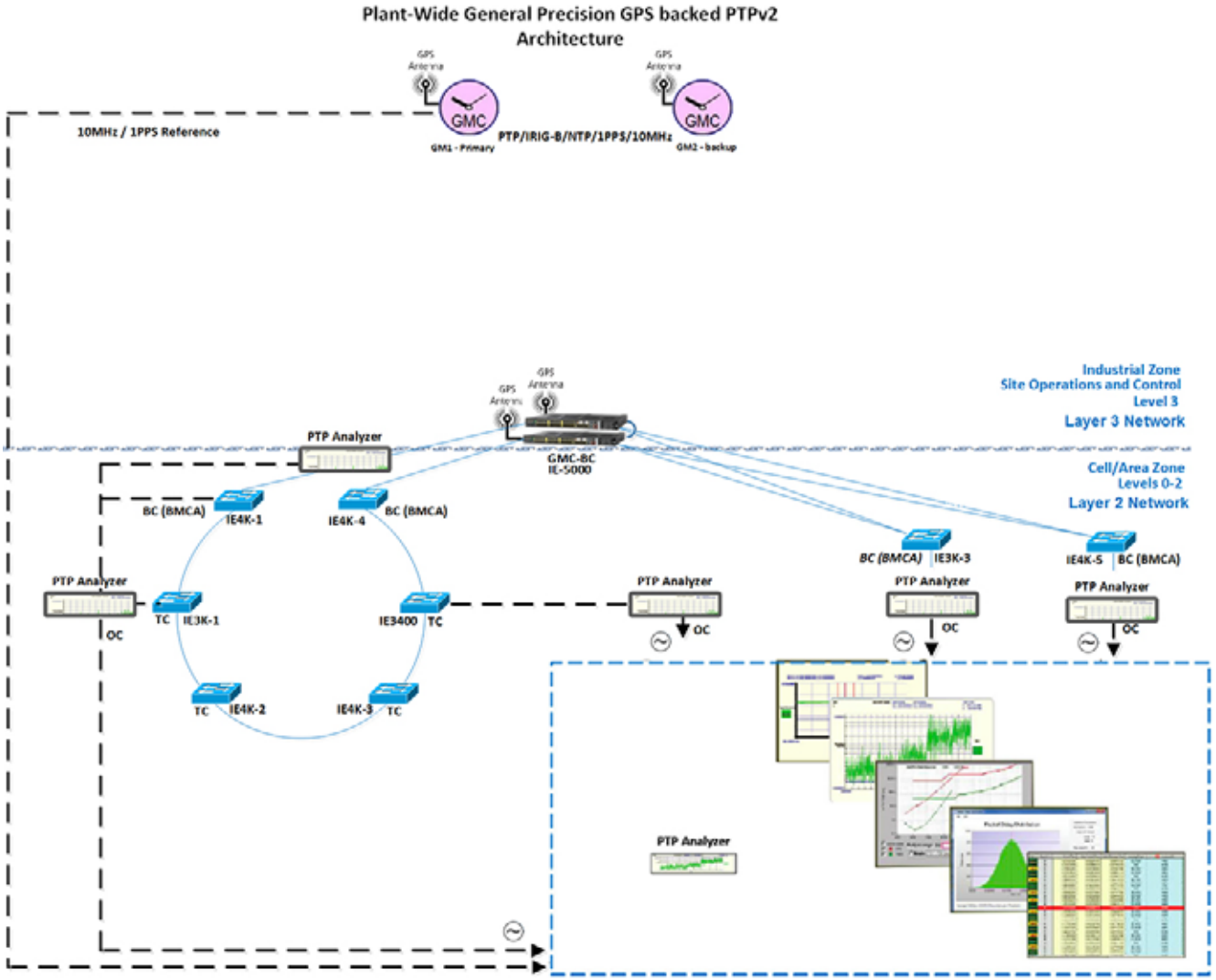
- Site-wide time distribution using Cisco IE 5000 as grandmaster

  Intermediate precision with distributed grandmaster clock design uses Cisco IE 5000 switch to directly connect to a GNSS source over industrial zone distribution switch. This design is targeted for general industrial operation where motion-related operation is not the main consideration when designing time synchronization distribution architecture.

  Intermediate precision with distributed grandmaster clock design inherits most of the high precision time distribution design by only removing the high precision dedicate grandmaster clock source located on the core network. The Cisco IE 5000 can either connect to a GNSS source or use the Cisco proprietary NTP-to-PTP (Flywheel) feature to assume the grandmaster clock role. It is not recommended to use an external internet NTP server if NTP-to-PTP grandmaster is a consideration in the PTP network design.

  Figure 43 shows the intermediate precision plantwide grandmaster clock architecture.

Figure 43 Plantwide Intermediate Precision GPS Backed PTPv2 Architecture



Where:

- Cisco IE 5000 pair switches connect to GNSS providing redundant plant-wide grandmaster clock.
- Cisco IE 4000 pair switches are configured as Boundary Clock (BC) on the top of each ring or start to dual-home to distribution switch pairs.
- Cisco IE 4000 is configured as end-to-end Transparent Clock (TC) inside ring.
- Cisco IE 3000 is configured as end-to-end TC inside ring.
- Cisco IE 3400 is configured as end-to-end TC inside ring.
- Customer PLC controller IP module is configured as Ordinary Clock (OC) to recover clock.
- Underlying resilience protocols vary with MSTP, REP, etc.
- Industrial Ethernet Switch is enabled with PTP-aware QoS for classifying and policing PTP messages.

Note: The Cisco Catalyst 9300 will support PTPv2 over VSS stacking in the future. Cisco IE 5000 stack-wise does not currently support PTP. In the topology in Figure 43, Cisco IE 5000 pairs are configured with HSRP over a Layer 2 trunk link.

The Cisco IE 5000 switch incorporated with stratum 3e Oven Controlled Crystal Oscillator (OCXO) can provide superior frequency stability in short term and high accuracy when in holdover state. High-precision Emerald OCXOs offer ±5 to ±8 ppb stability, 1 to 220 MHz frequency. It can be used as a drop-in replacement of legacy quartz OCXOs in emerging 5G and IEEE 1588 synchronization applications while improving overall system performance and robustness.

- Site-wide time distribution using IACS Time Module

  Refer to site-wide time distribution using Rockwell Automation PLCs:

  - Deploying Scalable Time Distribution within a Converged Plantwide Ethernet Architecture Design Guide https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/STD/DIG/CPwE-5-1-STD-DIG.html
  - Scalable Time Distribution within a Converged Plantwide Ethernet Architecture White Paper https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/STD/WP/CPwE-5-1-STD-WP.html

The following section provides a detailed configuration and limitation example for a third-party grandmaster clock and Industrial Ethernet switch (IES).

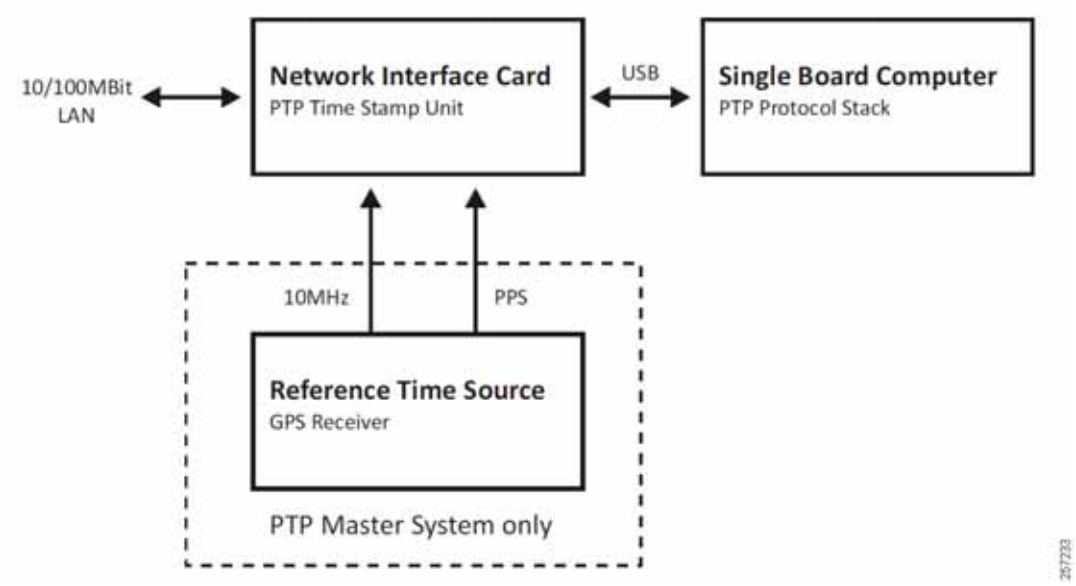
Configuring Meinberg LANTIME M600

Meinberg LANTIME M600 will provision PTP/NTP service from the core network (Purdue model level 3 above) as close as possible to the distribution network (Purdue model level 3) which connects the Cell/Area Zone. This can reduce PTP hop count and possible routing asymmetry. M600 is configure with IPv4/UDP multicast master with End-to-End(E2E) default profile, where UDP port 319/320 pairs will be used for PTP Event messages (for example: E2E default Profile: Sync/Delay_Req) and PTP general messages (Delay_Resp/Follow_UP): https://www.meinbergglobal.com/download/docs/manuals/english/ltos_6-24.pdf

Meinberg LANTIME M600 PTP Timestamping for Grandmaster Clock

M600 consists of three functional blocks: GPS reference time source will integrate with single board PTP computer via internal USB (169 NET) to get timestamping, PTP messages will be advertised via PTP timestamp unit via IP.

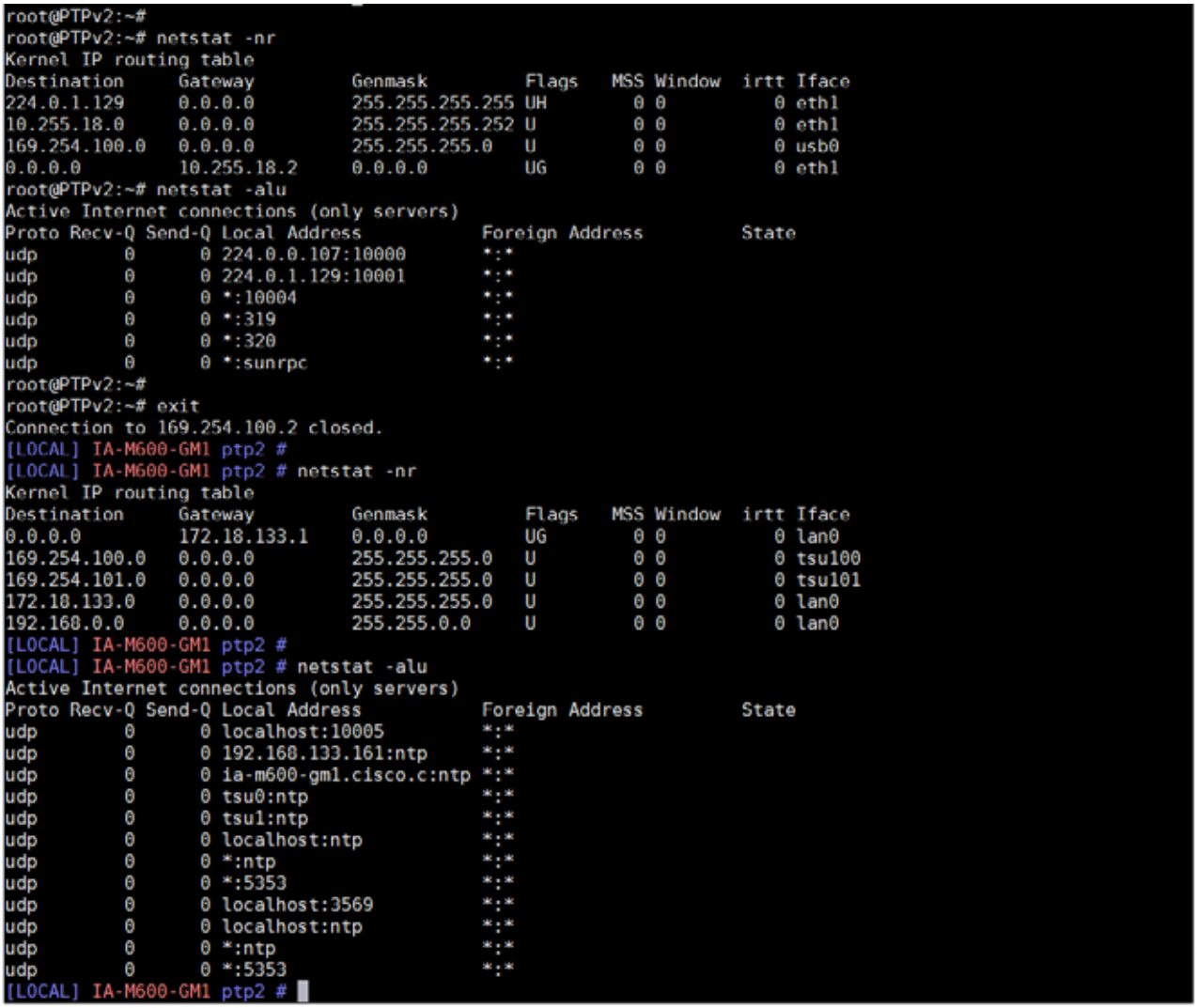
Figure 44 M600 Block Diagram



M600 PTP Timestamping

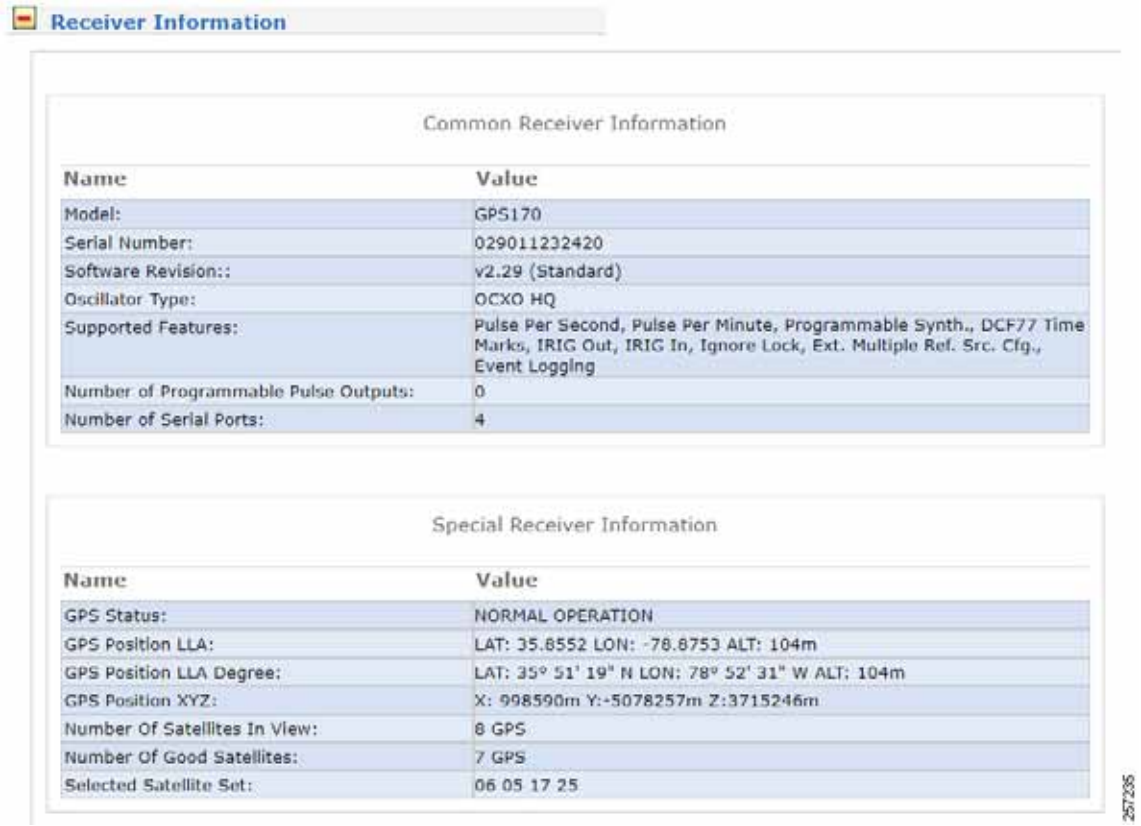
PTP messages transport over UDP port 319 and 320 via multicast addresses 224.0.0.107 and 224.0.0.129. This is handled via M600 single onboard computer. PTP messages advertise through manually configured 10 NET via external Fast Ethernet port as shown in Figure 45.

Figure 45 M600 Timestamping



M600 PTP User Interface Configuration

Figure 46 PTP GPS Status



Receiver Information

Common Receiver Information

Name	Value
Model:	GPS170
Serial Number:	029011232420
Software Revision::	v2.29 (Standard)
Oscillator Type:	OCXO HQ
Supported Features:	Pulse Per Second, Pulse Per Minute, Programmable Synth., DCF77 Time Marks, IRIG Out, IRIG In, Ignore Lock, Ext. Multiple Ref. Src. Cfg., Event Logging
Number of Programmable Pulse Outputs:	0
Number of Serial Ports:	4

Special Receiver Information

Name	Value
GPS Status:	NORMAL OPERATION
GPS Position LLA:	LAT: 35.8552 LON: -78.8753 ALT: 104m
GPS Position LLA Degree:	LAT: 35° 51' 19" N LON: 78° 52' 31" W ALT: 104m
GPS Position XYZ:	X: 998590m Y:-5078257m Z:3715246m
Number Of Satellites In View:	8 GPS
Number Of Good Satellites:	7 GPS
Selected Satellite Set:	06 05 17 25

257235

Figure 47 PTP Input Source Priority

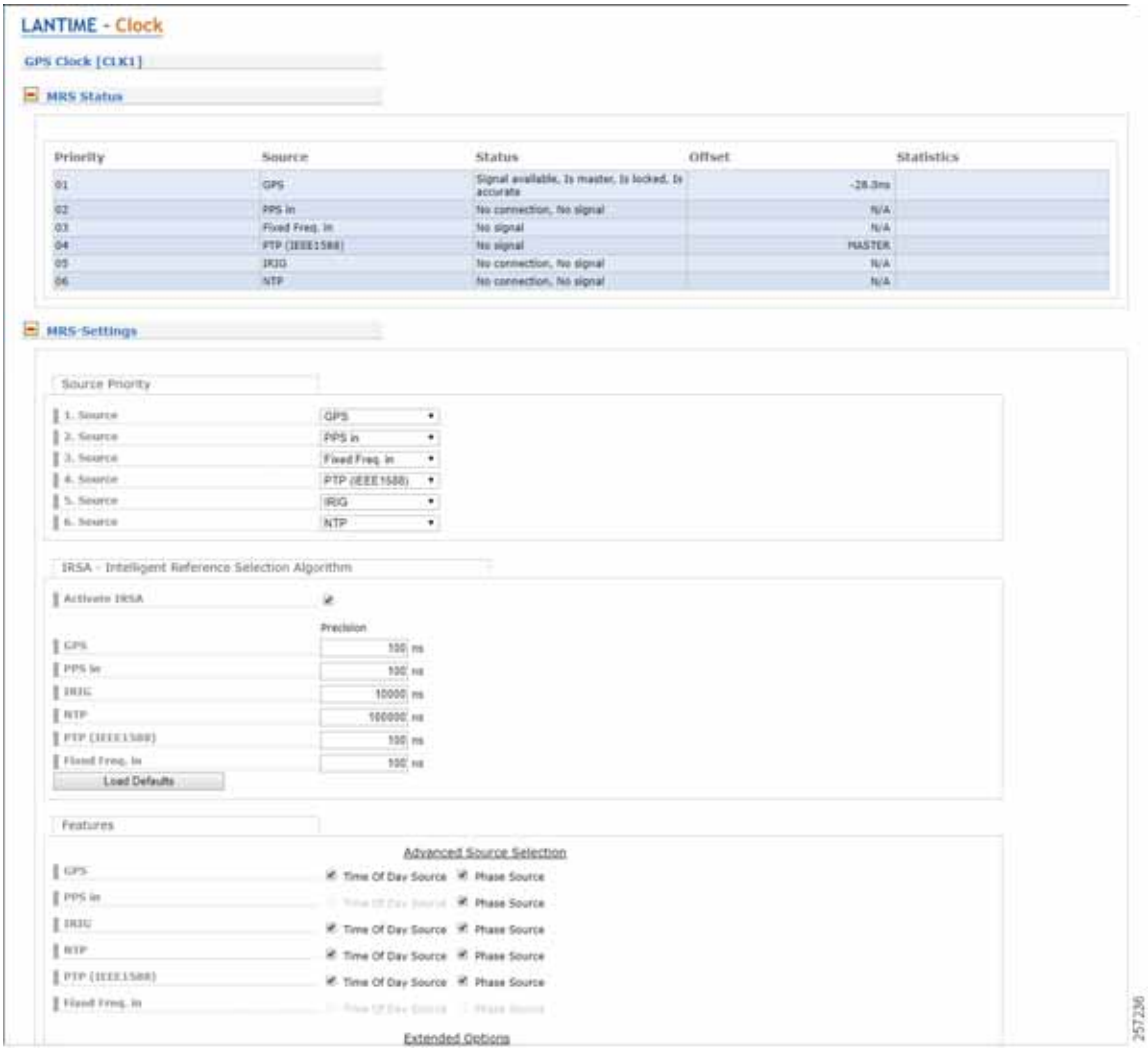


Figure 48 PTP Parameters–1

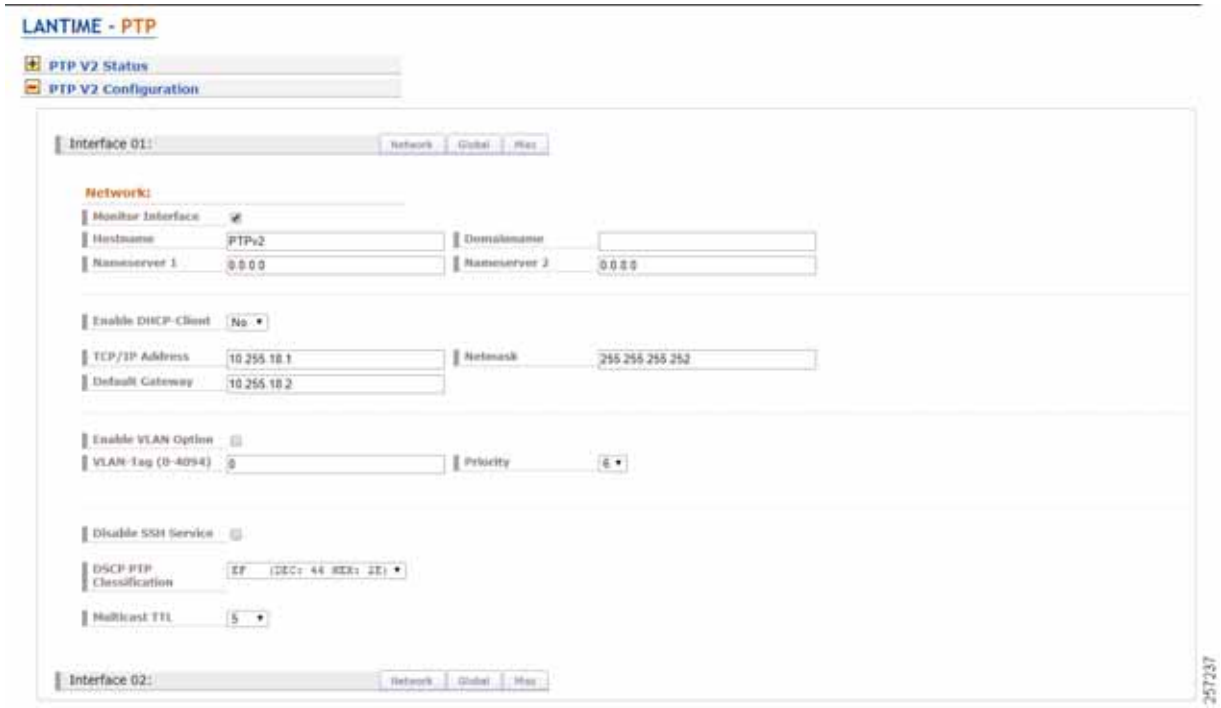
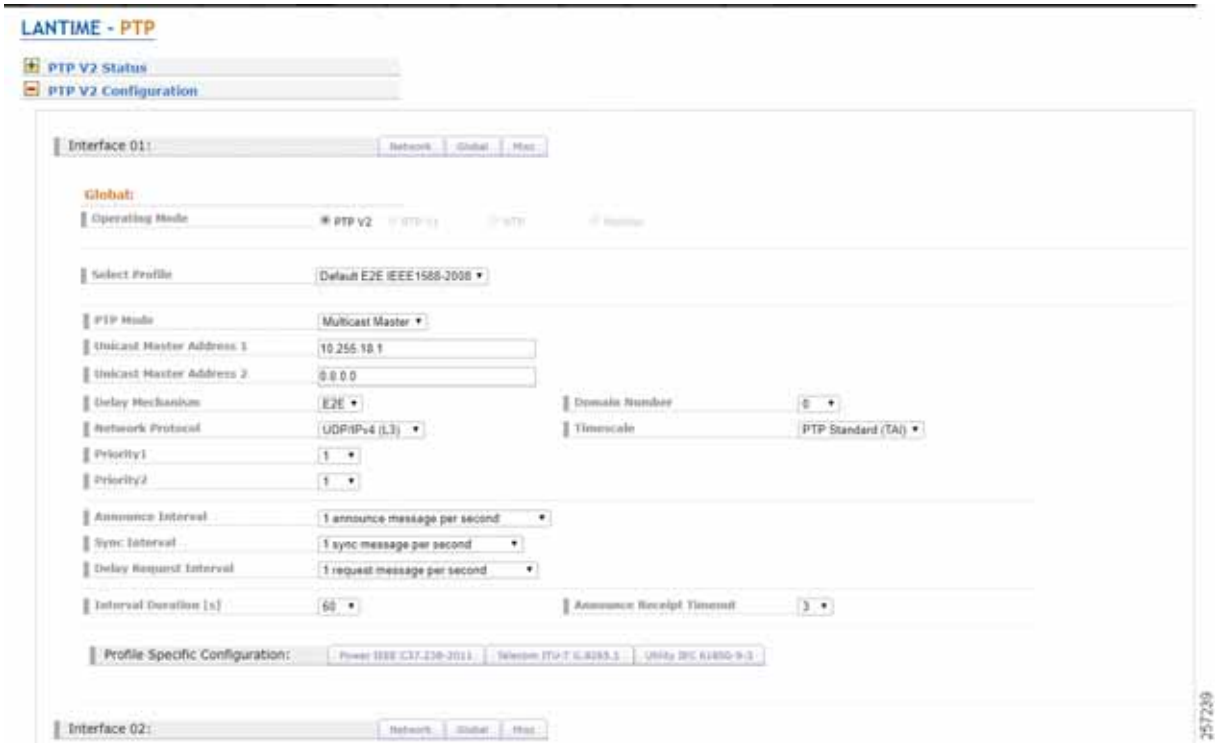


Figure 49 PTP Parameters–2



Configuring Cisco Catalyst 9300

Cisco Catalyst 9300 PTP Configuration Guide:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/16-9/configuration_guide/lyr2/b_169_lyr2_9300_cg/configuring_precision_time_protocol__ptp_.pdf

Restrictions and Limitations for PTP

- The output of show clock on the device and PTP servo clock displayed in **show platform software fed switch active PTP domain 0** are not synchronized to each other. These are two different clocks used on the switch.
- Inter-VLAN is not supported in PTP Transparent Clock Mode.
- PTP is supported only on the first 16 downlink ports and on all the uplink ports of the C9300-48UXM switch model.
- PTP is not supported in stacked systems.
- PTP is not supported on Layer 3 interface (support will be on release 16.12); currently SVI interface will be supported.
- The switch supports IEEE802.1AS and IEEE1588 default profile and they are mutually exclusive. Only one profile can be enabled on the switch at a time.
- We do not recommend having non-PTP enabled devices in the PTP network since it decreases clock synchronization accuracy.
- Management and signaling messages are not supported in Cisco IOS XE Fuji 16.8.1a. These messages are dropped in the switch without being processed.
- Moving from one PTP mode to the other is not recommended. Clear the existing mode using no PTP mode and then configure a new mode.
- IPv6, VRF, EtherChannel interface, and native Layer 3 ports are not supported

Cisco Catalyst 9300 PTP Default Profile Boundary Clock Configuration

The Cisco Catalyst 9300 is deployed on the enterprise core network to facilitate plantwide high precision grandmaster clock delivering time synchronization services across whole plant, where GM1 and backup GM2 are directly connected to a Cisco Catalyst 9300 core switch. The Cisco Catalyst 9300 will be configured in Boundary Clock (BC) mode to recover clock and regenerate clock for downstream PTP devices.

Table 4 Cisco Catalyst 9300 PTP Default Profile Boundary Clock Configuration

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	
	`Device> enable`
		Enables privileged EXEC mode.
		
		Enter your password if prompted.

Step 2	`Configure terminal`
	
	Example:
	
	`Device#configure terminal`
		Enter global configuration mode.

Step 3	`ptp transport ipv4 udp`
	`ptp mode boundary delay-req`
	`ptp priority1 <Value>`
	`ptp priority2 <Value>`
	
	Example:
	
	`Device(config)# ptp transport ipv4 udp`
	`Device(config)# ptp mode boundary delay-req`
	`Device(config)# ptp priority1 ppp`
	`Device(config)# ptp priority2 qqq`
		Specifies the synchronization transport mode, clock mode, and clock domain:
		
		■ boundary—Mode to enable the switch to participate in selecting the best primary clock. If no better clocks are detected, the switch becomes the grandmaster clock on the network and the parent clock to all connected devices. If the best primary is determined to be a clock connected to the switch, the switch synchronizes to that clock as a child to the clock, then acts as a parent clock to devices connected to other ports. After initial synchronization, the switch and the connected devices exchange timing messages to correct time skew caused by clock offsets and network delays. Use this mode when overload or heavy load conditions produce significant delay jitter.
		
		■ Once PTP default profile is enabled globally on the device, PTP is enabled on all the interfaces. To disable PTP selectively on individual interfaces, use the **no ptp enable** command under interface configuration.
		
		■ PTP priority1 and priority2

Step 4	`ptp vlan <Value>`
	
	Example:
	
	`Device(config)#interface vlan nnn`
	`Device(config)#ip address m.m.m.m n.n.n.n`
	`Device(config)#interface GigabitEthernetx/y/z`
	`Device(config-if)#switch mode trunk`
	`Device(config-if)#switch trunk allow vlan nnn`
	`Device(config-if)#ptp vlan nnn`
		Specify PTP over SVI:
		
		■ Within the PTP default profile, PTP messages are processed in VLAN 1 by default. Use the **ptp vlan vlan-name** command under interface configurations to allow PTP message processing on specific VLAN.
		
		You must add this to the VLAN database of the device.

Cisco Catalyst 9300 PTP Default Profile Boundary Clock Configuration Example

```
### PTP Boundary Clock ###
P5-9300-2#show run | sec ptp
ptp transport ipv4 udp
ptp mode boundary delay-req
ptp priority1 10
ptp priority2 11
 ptp vlan 118
P5-9300-2# P5-9300-2#
```

```
P5-9300-2#show run int gi1/0/48
Building configuration...

Current configuration : 228 bytes
!
interface GigabitEthernet1/0/48
 description Connect to Meinberg LANTIME M600-GM1 PTP
 no switchport
 ip address 10.255.18.2 255.255.255.252
 service-policy input CIP-PTP-Traffic
 service-policy output PTP-Event-Priority
end

P5-9300-2#show run int gi1/0/47
Building configuration...

Current configuration : 249 bytes
!
interface GigabitEthernet1/0/47
 description Connect to DEVICE Gi1/12 (PTP Static Path)
 switchport trunk allowed vlan 1,118
 switchport mode trunk
 ptp vlan 118
 service-policy input CIP-PTP-Traffic
 service-policy output PTP-Event-Priority
end

P5-9300-2#
P5-9300-2#show run int vlan 118
Building configuration...

Current configuration : 103 bytes
!
interface Vlan118
 ip address 10.255.18.6 255.255.255.252
 service-policy input CIP-PTP-Traffic
end
P5-9300-2#P5-9300-2#show ver | inc RELEASE SOFTWARE
Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.9.2, RELEASE SOFTWARE
(fc4)
BOOTLDR: System Bootstrap, Version 16.10.1r[FC1], RELEASE SOFTWARE (P)
P5-9300-2#
P5-9300-2#show run | sec ptp
ptp transport ipv4 udp
ptp mode boundary delay-req
ptp priority1 10
ptp priority2 11
 ptp vlan 118
P5-9300-2#
P5-9300-2#show ptp brief | inc 48|MASTER|SLAVE
GigabitEthernet1/0/7            0         MASTER
GigabitEthernet1/0/8            0         MASTER
GigabitEthernet1/0/9            0         MASTER
GigabitEthernet1/0/10           0         MASTER
GigabitEthernet1/0/46           0         MASTER
GigabitEthernet1/0/47           0         MASTER
GigabitEthernet1/0/48           0         SLAVE
TenGigabitEthernet1/1/1         0         MASTER
TenGigabitEthernet1/1/3         0         MASTER
TenGigabitEthernet1/1/5         0         MASTER
TenGigabitEthernet1/1/7         0         MASTER
TenGigabitEthernet1/1/8         0         MASTER
GigabitEthernet2/0/48           0         INITIALIZING
```

```
P5-9300-2#
P5-9300-2#show ptp parent
 PTP PARENT PROPERTIES
  Parent Clock:
  Parent Clock Identity: 0xEC:46:70:FF:FE:0:24:E4
  Parent Port Number: 1
  Observed Parent Offset (log variance): 17258
  Observed Parent Clock Phase Change Rate: N/A

  Grandmaster Clock:
  Grandmaster Clock Identity: 0xEC:46:70:FF:FE:0:24:E4
  Grandmaster Clock Quality:
        Class: 6
        Accuracy: Within 100ns
        Offset (log variance): 13563
        Priority1: 1
        Priority2: 1

P5-9300-2#
P5-9300-2#show ptp port gigabitEthernet 1/0/48
 PTP PORT DATASET: GigabitEthernet1/0/48
  Port identity: clock identity: 0x0:BC:60:FF:FE:AD:A5:0
  Port identity: port number: 48
  PTP version: 2
  Port state: SLAVE
  Delay request interval(log mean): 0
  Announce receipt time out: 3
  Announce interval(log mean): 0
  Sync interval(log mean): 0
  Delay Mechanism: End to End
  Peer delay request interval(log mean): 0
  Sync fault limit: 500000000

P5-9300-2#
P5-9300-2#show ptp port gigabitEthernet 1/0/47
 PTP PORT DATASET: GigabitEthernet1/0/47
  Port identity: clock identity: 0x0:BC:60:FF:FE:AD:A5:0
  Port identity: port number: 47
  PTP version: 2
  Port state: MASTER
  Delay request interval(log mean): 0
  Announce receipt time out: 3
  Announce interval(log mean): 0
  Sync interval(log mean): 0
  Delay Mechanism: End to End
  Peer delay request interval(log mean): 0
  Sync fault limit: 500000000
  Port VLAN Id: 118

P5-9300-2#
P5-9300-2#show ptp time-property
 PTP CLOCK TIME PROPERTY
  Current UTC offset valid: TRUE
  Current UTC offset: 37
  Leap 59: FALSE
  Leap 61: FALSE
  Time Traceable: TRUE
  Frequency Traceable: TRUE
  PTP Timescale: TRUE
  Time Source: GPS
  Time Property Persistence: 300 seconds

P5-9300-2#
P5-9300-2#show ptp clock
 PTP CLOCK INFO
```

```
  PTP Device Type: Boundary clock
  PTP Device Profile: Default Profile
  Clock Identity: 0x0:BC:60:FF:FE:AD:A5:0
  Clock Domain: 0
  Network Transport Protocol: udp-ipv4
  Number of PTP ports: 64
  Priority1: 10
  Priority2: 11
  Clock Quality:
        Class: 248
        Accuracy: Unknown
        Offset (log variance): 17258
  Offset From Master(ns): 0
  Mean Path Delay(ns): 115
  Steps Removed: 1

P5-9300-2#
P5-9300-2#
P5-9300-2#show platform software fed switch active ptp domain 0
Displaying data for domain number 0
=====================================

Profile Type : DEFAULT
Profile State: enabled
Clock Mode : BOUNDARY CLOCK
Delay Mechanism: : END-TO-END
PTP clock : 2019-5-24 17:45:57
mean_path_delay 113 nanoseconds
Transport Method : udp-ipv4

P5-9300-2#
```

Note: The Cisco Catalyst 9300 PTP default profile only supports Layer 2 in the released software, adding SVI configure.

Configuring Cisco IE 5000

Cisco IE 5000 PTP Configuration Guide:

- https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie4000/software/release/15-2_4_e/b_ptp_ie4k.pdf
- https://www.cisco.com/c/en/us/td/docs/switches/connectedgrid/cg-switch-sw-master/software/configuration/guide/gnss/b_gnss.html

Restrictions and Limitations for PTP

PTP Messages

- The Cisco PTP implementation supports only the two-step clock and not the one-step clock. If the switch receives a one-step message from the grandmaster clock, it will convert it into a two-step message.
- Cisco PTP supports multicast PTP messages only.

PTP Mode and Profile

- The switch and the grandmaster clock must be in the same PTP domain.
- In Default Profile mode, only the delay_request mechanism is supported. To change to Boundary Clock Mode with the delay_request mechanism, enter the **ptp mode boundary delay-req** command.

Packet Format

- The packet format for PTP messages can be 802.1q tagged packets or untagged packets.

- The switch does not support 802.1q QinQ tunneling.
- Subordinate IEDs must support tagged and untagged packets.
- When PTP packets are sent on the native VLAN in E2E Transparent Clock Mode, they are sent as untagged packets. To configure the switch to send them as tagged packets, enter the **global vlan dot1q tag native** command.

VLAN Configuration

- Set the PTP VLAN on a trunk port. The range is from 1 to 4094. The default is the native VLAN of the trunk port.
- In boundary mode, only PTP packets in PTP VLAN will be processed. PTP packets from other VLANs will be dropped.
- Before configuring the PTP VLAN on an interface, the PTP VLAN must be created and allowed on the trunk port.
- Most grandmaster clocks use the default VLAN 0. In Power Profile mode, the switch default VLAN is VLAN 1 and VLAN 0 is reserved. When you change the default grandmaster clock VLAN, it must be changed to a VLAN other than 0.
- When VLAN is disabled on the grandmaster clock, the PTP interface must be configured as an access port.

Clock Configuration

- All PHY PTP clocks are synchronized to the grandmaster clock. The switch system clock is not synchronized as part of PTP configuration and processes.
- When VLAN is enabled on the grandmaster clock, it must be in the same VLAN as the native VLAN of the PTP port on the switch.
- Grandmaster clocks can drop untagged PTP messages when a VLAN is configured on the grandmaster clock. To force the switch to send tagged packets to the grandmaster clock, enter the **global vlan dot1q tag native** command.

Clock Modes

- Boundary Clock Mode
  - You can enable this mode when the switch is in Power Profile Mode (Layer 2) or in Default Profile Mode (Layer 3).
- Forward Mode
  - You can enable this mode when the switch is in Power Profile Mode (Layer 2) or in Default Profile Mode (Layer 3).
  - When the switch is in Forward mode, the only global configuration available is the CLI command to switch to a different PTP mode (that is, boundary, e2etransparent, or p2ptransparent).
- E2E Transparent Clock Mode
  - You can enable this mode only when the switch is in Default Profile Mode (Layer 3).
  - When the switch is in E2E Transparent mode, the only global configuration available is the CLI command to switch to a different PTP mode (that is, boundary, p2ptransparent, or forward).
- P2P Transparent Clock Mode
  - You can enable this mode only when the switch is in Power Profile Mode (Layer 2).
  - When the switch is in P2P Transparent mode, the only global configuration available is the CLI command to switch to a different PTP mode (that is, boundary, e2etransparent, or forward).
- GMC-BC Clock Mode
  - You can enable this mode only when the switch is in Default Profile Mode.

PDV Filtering

- Adaptive mode (ptp transfer filter adaptive) is not available in Power Profile mode or 802.1AS profile mode.

PTP Interaction with Other Features

- The following PTP clock modes do not support EtherChannels:
  - e2etransparent
  - p2ptransparent
  - boundary
  - gmc-bc
- The following PTP clock modes only operate on a single VLAN:
  - e2etransparent
  - p2ptransparent

NTP to PTP Conversion

- The NTP to PTP feature supports the Default E2E Profile only.

Default Settings

- PTP is enabled on the switch by default.
- By default, the switch uses configuration values defined in the Default Profile (Default Profile mode is enabled).
- The switch default PTP clock mode is E2E Transparent Clock Mode.
- The default BC synchronization algorithm is linear filter.

GNSS Hardware

The Cisco IE 5000 uses a GNSS receiver with precise frequency and phase outputs for the host system. When connected to an external GNSS antenna, the receiver contains all the circuitry necessary to automatically acquire GNSS satellite signals, track up to 32 GNSS satellites, and compute location, speed, heading, and time. It provides an accurate one pulse-per-second (PPS) and stable 10 MHz frequency output.

The GNSS chip supports the following frequency bands:

- GPS/NAVSTAR–Global Positioning System-USA: L1
- GLONASS–Global'naya Navigatsionnaya Sputnikovaya Sistema-Russia: L1/G1
- BeiDou–China (including B1-2)

Note: The Galileo satellite system is not currently supported in the released software.

Table 5 Cisco IE 5000 PTP Default Profile Grandmaster Clock Configuration

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	
	`Device> enable`
		Enables privileged EXEC mode.
		
		Enter your password if prompted.

Table 5 Cisco IE 5000 PTP Default Profile Grandmaster Clock Configuration (continued)

Step 2	`Configure terminal`
	
	Example:
	
	`Device#configure terminal`
		Enter global configuration mode.

Table 5 Cisco IE 5000 PTP Default Profile Grandmaster Clock Configuration (continued)

Step 3	gnss antenna cable-delay 500 antenna power 3.3 Example: DEVICE(config-gnss)#gnss DEVICE(config-gnss)#antenna cable-delay 500 DEVICE(config-gnss)#constellation gps DEVICE(config-gnss)#antenna power 3.3 DEVICE(config-gnss)#anti-jam DEVICE(config-gnss)#end	Specifies GNSS parameters: antenna cable-delay, power, constellation, etc. There are two stages in the process for the GNSS receiver to acquire satellites and provide timing signals to the host system: ■ Self-Survey Mode—On reset, the GNSS receiver comes up in self-survey mode and attempts to lock on to a minimum of four different satellites to obtain a 3-D fix on its current position. It computes nearly 2000 different positions for these satellites, which takes about 35 minutes. Also during this stage, the GNSS receiver is able to generate accurate timing signals and achieve "Normal (Locked to GPS)" state. Note that the timing signal obtained during self-survey mode can be off by 20 seconds; therefore, Cisco IOS collects PPS only during OD mode. After the self-survey is complete, the results are saved to the GNSS receiver flash, which speeds up the transition to OD mode the next time the self-survey runs. You can manually restart the self-survey process with the **gnss self-survey restart** Cisco IOS command. After self-survey mode completes again, the results in the GNSS receiver flash are overwritten with the updated results. ■ Over-determined (OD) clock mode—The device transitions to OD mode when self-survey mode is completed and the position information is stored in non-volatile memory on the device. In this mode, the GNSS receiver outputs timing information based on satellite positions obtained in self-survey mode. The GNSS receiver remains in OD mode until there is a reason to leave it, such as: ■ Detection of a position relocation of the antenna of more than 100m, which triggers an automatic restart of the self-survey. ■ Manual restart of the self-survey using the **gnss self-survey restart** command. Self-survey takes about 30 minutes to finish as shown below: May 24 12:52:33.168 EDT: %GNSS-5-GNSS_SELF_SURVEY_COMPLETE: self-survey complete May 24 12:52:33.168 EDT: %GNSS-5-GNSS_IN_OD_MODE: in OD mode May 24 12:52:37.177 EDT: %GNSS-5-GNSS_ANTENNA_UP: 1PPS is UP … May 24 13:27:04.169 EDT: %GNSS-5-GNSS_SELF_SURVEY_COMPLETE: self-survey complete May 24 13:27:04.169 EDT: %GNSS-5-GNSS_IN_OD_MODE: in OD mode May 24 13:27:04.169 EDT: %GNSS-5-GNSS_ANTENNA_UP: 1PPS is UP

Table 5 Cisco IE 5000 PTP Default Profile Grandmaster Clock Configuration (continued)

Step 4	`ptp mode gmc-bc delay-req`
	`ptp transfer feedforward`
	`ptp priority1 <value>`
	`ptp priority2 <value>`
	
	Example:
	
	`Device(config)# ptp mode gmc-bc delay-req`
	`Device(config)# ptp transfer feedforward`
	`Device(config)# ptp priority1 ppp`
	`Device(config)# ptp priority2 qqq`
		Specifies the synchronization transport mode, clock mode, and clock domain:
		
		■ gmc-bc—The GMC-BC acts like a BC, which is a multi-port device, with a single-port GMC connected to a virtual port on the BC. The GMC-BC switches between acting like a GMC when the GMC-BC is the primary GMC, and acting like a BC when the GMC-BC is a backup. This ensures that all devices on the PTP network remain synchronized in a failover scenario.
		
		■ feedforward—Very fast and accurate. No PDV filtering.
		
		■ PTP priority1 and priority2

Cisco IE 5000 PTP Default Profile Grandmaster Clock Configuration Example

```
IE5K-1#show run | sec gnss
gnss
 antenna cable-delay 500
 antenna power 3.3
IE5K-1#
IE5K-1#show run | sec ptp
ptp mode gmc-bc delay-req
ptp priority1 100
ptp priority2 101
ptp transfer feedforward
IE5K-1#

IE5K-1#show run int gi1/20
Building configuration...

Current configuration : 389 bytes
!
interface GigabitEthernet1/20
 description Connect to IAPTP-IE4K-01 Gig 1/1
 switchport trunk allowed vlan 10,11,18,19,21,901,918-920
 switchport trunk native vlan 901
 switchport mode trunk
 load-interval 30
 rep segment 15 edge primary
 alarm profile ab-alarm
 spanning-tree link-type point-to-point
 service-policy input CIP-PTP-Traffic
 service-policy output PTP-Event-Priority
end

IE5K-1#show run int gi1/17
Building configuration...

Current configuration : 370 bytes
!
interface GigabitEthernet1/17
 description Connect IE5K-2 IAPTP-HSRP-PO10 Gi1/17
 switchport trunk allowed vlan 10,11,18,19,21,901,917-920
 switchport trunk native vlan 917
 switchport mode trunk
 load-interval 30
 rep segment 17 edge primary
 spanning-tree link-type point-to-point
```

```
 service-policy input CIP-PTP-Traffic
 service-policy output PTP-Event-Priority
end

IE5K-1#show run int gi1/18
Building configuration...

Current configuration : 362 bytes
!
interface GigabitEthernet1/18
 description Connect IE5K-2 IAPTP-HSRP-PO10 Gi1/17
 switchport trunk allowed vlan 10,11,18,19,21,901,917-920
 switchport trunk native vlan 917
 switchport mode trunk
 load-interval 30
 rep segment 17 edge
 spanning-tree link-type point-to-point
 service-policy input CIP-PTP-Traffic
 service-policy output PTP-Event-Priority
end

IE5K-1#IE5K-1#show ver | inc RELEASE SOFTWARE|Version|image
Cisco IOS Software, IE5000  Software (IE5000-UNIVERSALK9-M), Experimental Version 15.2(20190515:094847)
[vadasser-7_e_rep 117]
BOOTLDR: IE5000  Boot Loader (IE5000-HBOOT-M) Version 15.2(2r)EB, RELEASE SOFTWARE (fc1)
System image file is "sdflash:ie5000-universalk9-mz_backedout_CSCvd47399.SPA"
Version ID                      : V06
Switch Ports Model                      SW Version            SW Image
IE5K-1#
IE5K-1#show gnss status
 GNSS status: Enable
 Constellation: GPS
 Receiver Status: OD
 Survey progress: 100
 Satellite count: 7
 PDOP: 1.00    TDOP: 1.00
 HDOP: 0.00    VDOP: 0.00
 Alarm: None

IE5K-1#show gnss satellite all
SV Type Codes: 0 - GPS, 1 - GLONASS, 2 - Beidou

All Satellites Info:
SV PRN No   Channel No       Acq Flg    Ephemeris Flg     SV Type     Sig Strength
--------------------------------------------------------------------------------
        5            0             1                1           0               48
        2            1             1                1           0               45
       13            2             1                1           0               44
       29            3             1                1           0               48
       25            4             1                1           0               38
       15            5             1                1           0               45
       21            6             1                1           0               41
IE5K-1#show gnss time
Current GNSS Time:
Time: 2019/05/25  01:47:03 UTC Offset: 18
IE5K-1#show gnss location
Current GNSS Location:
  LOC: 35:51.314214449 N  78:52.518730299 W  92.77905 m
IE5K-1#show platform gnss
Board ID: 0x5000000 (Production SKU)
GNSS Chip:
  Hardware code: 3023 - RES SMT 360
  Serial Number: 1275127926
  Build Date: 6/24/2017
IE5K-1#
```

```
IE5K-1#show run | sec ptp
ptp mode gmc-bc delay-req
ptp priority1 100
ptp priority2 101
ptp transfer feedforward
IE5K-1#
IE5K-1#show ptp port | inc MASTER|SLAVE|PORT
 PTP PORT DATASET: GigabitEthernet1/1
  Port state: MASTER
 PTP PORT DATASET: GigabitEthernet1/2
  Port state: MASTER
 PTP PORT DATASET: GigabitEthernet1/3
  Port state: MASTER
 PTP PORT DATASET: GigabitEthernet1/4
  Port state: MASTER
 PTP PORT DATASET: GigabitEthernet1/5
 PTP PORT DATASET: GigabitEthernet1/6
 PTP PORT DATASET: GigabitEthernet1/7
 PTP PORT DATASET: GigabitEthernet1/8
 PTP PORT DATASET: GigabitEthernet1/9
 PTP PORT DATASET: GigabitEthernet1/10
 PTP PORT DATASET: GigabitEthernet1/11
 PTP PORT DATASET: GigabitEthernet1/12
 PTP PORT DATASET: GigabitEthernet1/13
 PTP PORT DATASET: GigabitEthernet1/14
 PTP PORT DATASET: GigabitEthernet1/15
 PTP PORT DATASET: GigabitEthernet1/16
  Port state: MASTER
 PTP PORT DATASET: GigabitEthernet1/17
  Port state: MASTER
 PTP PORT DATASET: GigabitEthernet1/18
  Port state: MASTER
 PTP PORT DATASET: GigabitEthernet1/19
  Port state: MASTER
 PTP PORT DATASET: GigabitEthernet1/20
  Port state: MASTER
 PTP PORT DATASET: GigabitEthernet1/21
 PTP PORT DATASET: GigabitEthernet1/22
 PTP PORT DATASET: GigabitEthernet1/23
 PTP PORT DATASET: GigabitEthernet1/24
 PTP PORT DATASET: GigabitEthernet1/25
 PTP PORT DATASET: GigabitEthernet1/26
 PTP PORT DATASET: GigabitEthernet1/27
 PTP PORT DATASET: GigabitEthernet1/28
IE5K-1#
IE5K-1#show ptp parent
 PTP PARENT PROPERTIES
  Parent Clock:
  Parent Clock Identity: 0xD4:E8:80:FF:FE:6:F2:0
  Parent Port Number: 0
  Observed Parent Offset (log variance): N/A
  Observed Parent Clock Phase Change Rate: N/A

  Grandmaster Clock:
  Grandmaster Clock Identity: 0xD4:E8:80:FF:FE:6:F2:0
  Grandmaster Clock Quality:
        Class: 6
        Accuracy: Within 250ns
        Offset (log variance): N/A
        Priority1: 100
        Priority2: 101
```

```
IE5K-1#show ptp cloc
 PTP CLOCK INFO
  PTP Device Type: Grand Master clock - Boundary clock
  PTP Device Profile: Default Profile
  Clock Identity: 0xD4:E8:80:FF:FE:6:F2:0
  Clock Domain: 0
  Number of PTP ports: 28
  Time Transfer: Feedforward
  Priority1: 100
  Priority2: 101
  Clock Quality:
        Class: 6
        Accuracy: Within 250ns
        Offset (log variance): N/A
  Offset From Master(ns): 0
  Mean Path Delay(ns): 0
  Steps Removed: 0
  Local clock time: 21:49:06 EDT May 24 2019

IE5K-1#show ptp time-property
 PTP CLOCK TIME PROPERTY
  Current UTC offset valid: TRUE
  Current UTC offset: 37
  Leap 59: FALSE
  Leap 61: FALSE
  Time Traceable: TRUE
  Frequency Traceable: TRUE
  PTP Timescale: TRUE
  Time Source: GNSS

IE5K-1#show ptp foreign-master-record
 PTP FOREIGN MASTER RECORDS
 Interface GigabitEthernet1/1
   Empty
 Interface GigabitEthernet1/2
   Empty
 Interface GigabitEthernet1/3
   Empty
 Interface GigabitEthernet1/4
   Empty
 Interface GigabitEthernet1/5
   Empty
 Interface GigabitEthernet1/6
   Empty
 Interface GigabitEthernet1/7
   Empty
 Interface GigabitEthernet1/8
   Empty
 Interface GigabitEthernet1/9
   Empty
 Interface GigabitEthernet1/10
   Empty
 Interface GigabitEthernet1/11
   Empty
 Interface GigabitEthernet1/12
   Empty
 Interface GigabitEthernet1/13
   Empty
 Interface GigabitEthernet1/14
   Empty
 Interface GigabitEthernet1/15
   Empty
 Interface GigabitEthernet1/16
   Empty
```

```
 Interface GigabitEthernet1/17
   Empty
 Interface GigabitEthernet1/18
   Empty
 Interface GigabitEthernet1/19
   Empty
 Interface GigabitEthernet1/20
   Empty
 Interface GigabitEthernet1/21
   Empty
 Interface GigabitEthernet1/22
   Empty
 Interface GigabitEthernet1/23
   Empty
 Interface GigabitEthernet1/24
   Empty
 Interface GigabitEthernet1/25
   Empty
 Interface GigabitEthernet1/26
   Empty
 Interface GigabitEthernet1/27
   Empty
 Interface GigabitEthernet1/28
   Empty
IE5K-1#
```

Table 6 Cisco IE 5000 PTP Default Profile Boundary Clock Configuration

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	
	`Device> enable`
		Enables privileged EXEC mode.
		
		Enter your password if prompted.

Table 6 Cisco IE 5000 PTP Default Profile Boundary Clock Configuration (continued)

Step 2	`Configure terminal`
	
	Example:
	
	`Device#configure terminal`
		Enter global configuration mode.

Step 3	`ptp mode boundary delay-req`
	`ptp time-property persist infinite`
	`ptp transfer feedforward`
	`ptp priority1 <value>`
	`ptp priority2 <value>`
	
	Example:
	
	`Device(config)# ptp mode boundary delay-req`
	`Device(config)# ptp time-property persist infinite`
	`Device(config)# ptp transfer feedforward`
	`Device(config)# ptp priority1 ppp`
	`Device(config)# ptp priority2 qqq`
		Specifies the synchronization transport mode, clock mode, and clock domain:
		
		■ boundary—Mode to enable the switch to participate in selecting the best primary clock. If no better clocks are detected, the switch becomes the grandmaster clock on the network and the parent clock to all connected devices. If the best primary is determined to be a clock connected to the switch, the switch synchronizes to that clock as a child to the clock, then acts as a parent clock to devices connected to other ports. After initial synchronization, the switch and the connected devices exchange timing messages to correct time skew caused by clock offsets and network delays. Use this mode when overload or heavy load conditions produce significant delay jitter.
		
		■ **PTP time property persist infinite** would preserve the time properties, preventing subordinate clocks from detecting a variance in the time values when the redundant grandmaster clock comes out of standby flapping.
		
		■ PTP priority1 and priority2

Step 4	`ptp vlan <value>`
	
	Example:
	
	`Device(config)#interface vlan nnn`
	`Device(config)#ip address m.m.m.m n.n.n.n`
	`Device(config)#interface GigabitEthernetx/y/z`
	`Device(config-if)#switch mode trunk`
	`Device(config-if)#switch trunk allow vlan nnn`
	`Device(config-if)#ptp vlan nnn`
		Specify PTP over SVI:
		
		■ Within PTP default profile, PTP messages are processed in VLAN 1 by default. Use **ptp vlan vlan-name** command under interface configurations to allow PTP message processing on specific VLAN.
		
		■ You must add this to the VLAN database of the device. PTP VLAN can only be configure after you apply PTP global configure.

Cisco IE 5000 PTP Default Profile Boundary Clock Configuration Example

```
DEVICE#show run | sec ptp
ptp mode boundary delay-req
ptp priority1 100
ptp priority2 101
ptp time-property persist infinite
ptp transfer feedforward
DEVICE#
DEVICE#show run int gi1/12
Building configuration...

Current configuration : 250 bytes
!
interface GigabitEthernet1/12
 description Connect to C9300-1 Gi1/0/47 (PTP Static Path)
 switchport trunk allowed vlan 1,118
```

```
 switchport mode trunk
 ptp vlan 118
 service-policy input CIP-PTP-Traffic
 service-policy output PTP-Event-Priority
end

DEVICE#show run int vlan 118
Building configuration...

Current configuration : 65 bytes
!
interface Vlan118
 ip address 10.255.18.5 255.255.255.252
end

DEVICE#show run int gi1/20
Building configuration...

Current configuration : 389 bytes
!
interface GigabitEthernet1/20
 description Connect to IAPTP-IE4K-01 Gig 1/1
 switchport trunk allowed vlan 10,11,18,19,21,901,918-920
 switchport trunk native vlan 901
 switchport mode trunk
 load-interval 30
 rep segment 15 edge primary
 alarm profile ab-alarm
 spanning-tree link-type point-to-point
 service-policy input CIP-PTP-Traffic
 service-policy output PTP-Event-Priority
end

DEVICE#
DEVICE#show run int gi1/17
Building configuration...

Current configuration : 370 bytes
!
interface GigabitEthernet1/17
 description Connect IE5K-2 IAPTP-HSRP-PO10 Gi1/17
 switchport trunk allowed vlan 10,11,18,19,21,901,917-920
 switchport trunk native vlan 917
 switchport mode trunk
 load-interval 30
 rep segment 17 edge primary
 spanning-tree link-type point-to-point
 service-policy input CIP-PTP-Traffic
 service-policy output PTP-Event-Priority
end

DEVICE#show run int gi1/18
Building configuration...

Current configuration : 362 bytes
!
interface GigabitEthernet1/18
 description Connect IE5K-2 IAPTP-HSRP-PO10 Gi1/17
 switchport trunk allowed vlan 10,11,18,19,21,901,917-920
 switchport trunk native vlan 917
 switchport mode trunk
 load-interval 30
 rep segment 17 edge
```

```
 spanning-tree link-type point-to-point
 service-policy input CIP-PTP-Traffic
 service-policy output PTP-Event-Priority
end

DEVICE#sDEVICE#show ver | inc RELEASE SOFTWARE|Version|image
Cisco IOS Software, IE5000  Software (IE5000-UNIVERSALK9-M), Experimental Version 15.2(20190515:094847)
[vadasser-7_e_rep 117]
BOOTLDR: IE5000  Boot Loader (IE5000-HBOOT-M) Version 15.2(2r)EB, RELEASE SOFTWARE (fc1)
System image file is "sdflash:ie5000-universalk9-mz_backedout_CSCvd47399.SPA"
Version ID                      : V06
Switch Ports Model                      SW Version            SW Image
DEVICE#
DEVICE#show run | sec ptp
ptp mode boundary delay-req
ptp priority1 100
ptp priority2 101
ptp time-property persist infinite
ptp transfer feedforward
DEVICE#
DEVICE#show ptp port | inc MASTER|SLAVE|PORT
 PTP PORT DATASET: GigabitEthernet1/1
 PTP PORT DATASET: GigabitEthernet1/2
  Port state: MASTER
 PTP PORT DATASET: GigabitEthernet1/3
  Port state: MASTER
 PTP PORT DATASET: GigabitEthernet1/4
  Port state: MASTER
 PTP PORT DATASET: GigabitEthernet1/5
 PTP PORT DATASET: GigabitEthernet1/6
 PTP PORT DATASET: GigabitEthernet1/7
 PTP PORT DATASET: GigabitEthernet1/8
 PTP PORT DATASET: GigabitEthernet1/9
 PTP PORT DATASET: GigabitEthernet1/10
 PTP PORT DATASET: GigabitEthernet1/11
 PTP PORT DATASET: GigabitEthernet1/12
  Port state: SLAVE
 PTP PORT DATASET: GigabitEthernet1/13
 PTP PORT DATASET: GigabitEthernet1/14
 PTP PORT DATASET: GigabitEthernet1/15
 PTP PORT DATASET: GigabitEthernet1/16
  Port state: MASTER
 PTP PORT DATASET: GigabitEthernet1/17
  Port state: MASTER
 PTP PORT DATASET: GigabitEthernet1/18
  Port state: MASTER
 PTP PORT DATASET: GigabitEthernet1/19
  Port state: MASTER
 PTP PORT DATASET: GigabitEthernet1/20
  Port state: MASTER
 PTP PORT DATASET: GigabitEthernet1/21
 PTP PORT DATASET: GigabitEthernet1/22
 PTP PORT DATASET: GigabitEthernet1/23
 PTP PORT DATASET: GigabitEthernet1/24
 PTP PORT DATASET: GigabitEthernet1/25
 PTP PORT DATASET: GigabitEthernet1/26
 PTP PORT DATASET: GigabitEthernet1/27
 PTP PORT DATASET: GigabitEthernet1/28
DEVICE#
DEVICE#show run int gi1/12
Building configuration...

Current configuration : 250 bytes
!
interface GigabitEthernet1/12
```

```
 description Connect to C9300-1 Gi1/0/47 (PTP Static Path)
 switchport trunk allowed vlan 1,118
 switchport mode trunk
 ptp vlan 118
 service-policy input CIP-PTP-Traffic
 service-policy output PTP-Event-Priority
end

DEVICE#show run int gi1/20
Building configuration...

Current configuration : 389 bytes
!
interface GigabitEthernet1/20
 description Connect to IAPTP-IE4K-01 Gig 1/1
 switchport trunk allowed vlan 10,11,18,19,21,901,918-920
 switchport trunk native vlan 901
 switchport mode trunk
 load-interval 30
 rep segment 15 edge primary
 alarm profile ab-alarm
 spanning-tree link-type point-to-point
 service-policy input CIP-PTP-Traffic
 service-policy output PTP-Event-Priority
end

DEVICE#show run int gi1/17
Building configuration...

Current configuration : 370 bytes
!
interface GigabitEthernet1/17
 description Connect IE5K-2 IAPTP-HSRP-PO10 Gi1/17
 switchport trunk allowed vlan 10,11,18,19,21,901,917-920
 switchport trunk native vlan 917
 switchport mode trunk
 load-interval 30
 rep segment 17 edge primary
 spanning-tree link-type point-to-point
 service-policy input CIP-PTP-Traffic
 service-policy output PTP-Event-Priority
end

DEVICE#show run int gi1/18
Building configuration...

Current configuration : 362 bytes
!
interface GigabitEthernet1/18
 description Connect IE5K-2 IAPTP-HSRP-PO10 Gi1/17
 switchport trunk allowed vlan 10,11,18,19,21,901,917-920
 switchport trunk native vlan 917
 switchport mode trunk
 load-interval 30
 rep segment 17 edge
 spanning-tree link-type point-to-point
 service-policy input CIP-PTP-Traffic
 service-policy output PTP-Event-Priority
end

DEVICE#
DEVICE#show ptp parent
 PTP PARENT PROPERTIES
```

```
  Parent Clock:
  Parent Clock Identity: 0x0:BC:60:FF:FE:AD:A5:0
  Parent Port Number: 47
  Observed Parent Offset (log variance): N/A
  Observed Parent Clock Phase Change Rate: N/A

  Grandmaster Clock:
  Grandmaster Clock Identity: 0xEC:46:70:FF:FE:0:24:E4
  Grandmaster Clock Quality:
        Class: 6
        Accuracy: Within 100ns
        Offset (log variance): 13563
        Priority1: 1
        Priority2: 1

DEVICE#show ptp clo
DEVICE#show ptp clock
 PTP CLOCK INFO
  PTP Device Type: Boundary clock
  PTP Device Profile: Default Profile
  Clock Identity: 0xD4:E8:80:FF:FE:6:F2:0
  Clock Domain: 0
  Number of PTP ports: 28
  Time Transfer: Feedforward
  Priority1: 100
  Priority2: 101
  Clock Quality:
        Class: 248
        Accuracy: Unknown
        Offset (log variance): N/A
  Offset From Master(ns): 8
  Mean Path Delay(ns): 147
  Steps Removed: 2
  Local clock time: 15:04:28 EDT May 24 2019

DEVICE#show ptp tim
DEVICE#show ptp time-property
 PTP CLOCK TIME PROPERTY
  Current UTC offset valid: TRUE
  Current UTC offset: 37
  Leap 59: FALSE
  Leap 61: FALSE
  Time Traceable: TRUE
  Frequency Traceable: TRUE
  PTP Timescale: TRUE
  Time Source: GNSS
  Time Property Persistence: Infinite

DEVICE#show ptp fo
DEVICE#show ptp foreign-master-record
 PTP FOREIGN MASTER RECORDS
 Interface GigabitEthernet1/1
   Empty
 Interface GigabitEthernet1/2
   Empty
 Interface GigabitEthernet1/3
   Empty
 Interface GigabitEthernet1/4
   Empty
 Interface GigabitEthernet1/5
   Empty
 Interface GigabitEthernet1/6
   Empty
 Interface GigabitEthernet1/7
   Empty
```

```
 Interface GigabitEthernet1/8
   Empty
 Interface GigabitEthernet1/9
   Empty
 Interface GigabitEthernet1/10
   Empty
 Interface GigabitEthernet1/11
   Empty
 Interface GigabitEthernet1/12
   Foreign master port identity: clock id: 0x0:BC:60:FF:FE:AD:A5:0
   Foreign master port identity: port num: 47
   Number of Announce messages: 3
   Message received port: 12
   Time stamps: 145448162, 145447166
 Interface GigabitEthernet1/13
   Empty
 Interface GigabitEthernet1/14
   Empty
 Interface GigabitEthernet1/15
   Empty
 Interface GigabitEthernet1/16
   Empty
 Interface GigabitEthernet1/17
   Empty
 Interface GigabitEthernet1/18
   Empty
 Interface GigabitEthernet1/19
   Empty
 Interface GigabitEthernet1/20
   Empty
 Interface GigabitEthernet1/21
   Empty
 Interface GigabitEthernet1/22
   Empty
 Interface GigabitEthernet1/23
   Empty
 Interface GigabitEthernet1/24
   Empty
 Interface GigabitEthernet1/25
   Empty
 Interface GigabitEthernet1/26
   Empty
 Interface GigabitEthernet1/27
   Empty
 Interface GigabitEthernet1/28
   Empty
DEVICE#
```

Note: The Cisco Catalyst 9300 PTP default profile only supports Layer 2 in the released software, adding SVI configure.

Configuring Cisco IE 4000

For the Cisco IE 4000 PTP Configuration Guide and Restrictions and Limitations for PTP, refer to Configuring Cisco IE 5000, page 103.

Table 7 Cisco IE 4000 PTP Default Profile Boundary Clock

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	
	`Device> enable`
		Enables privileged EXEC mode.
		
		Enter your password if prompted.

Step 2	`Configure terminal`
	
	Example:
	
	`Device#configure terminal`
		Enter global configuration mode.

Step 3	`ptp mode boundary delay-req`
	`ptp time-property persist infinite`
	`ptp transfer feedforward`
	`ptp priority1 <value>`
	`ptp priority2 <value>`
	
	Example:
	
	`Device(config)# ptp mode boundary delay-req`
	`Device(config)# ptp time-property persist infinite`
	`Device(config)# ptp transfer feedforward`
	`Device(config)# ptp priority1 ppp`
	`Device(config)# ptp priority2 qqq`
		Specifies the synchronization transport mode, clock mode, and clock domain:
		
		■ boundary—Mode to enable the switch to participate in selecting the best primary clock. If no better clocks are detected, the switch becomes the grandmaster clock on the network and the parent clock to all connected devices. If the best primary is determined to be a clock connected to the switch, the switch synchronizes to that clock as a child to the clock, then acts as a parent clock to devices connected to other ports. After initial synchronization, the switch and the connected devices exchange timing messages to correct time skew caused by clock offsets and network delays. Use this mode when overload or heavy load conditions produce significant delay jitter.
		
		■ **PTP time property persist infinite** would preserve the time properties, preventing subordinate clocks from detecting a variance in the time values when the redundant grandmaster clock comes out of standby flapping.
		
		■ PTP priority1 and priority2

Cisco IE 4000 PTP Default Profile Boundary Clock Configuration Example

```
IAPTP-IE4K-01#show run | sec ptp
ptp mode boundary delay-req
ptp priority1 110
ptp priority2 111
ptp time-property persist infinite
ptp transfer feedforward
IAPTP-IE4K-01#
IAPTP-IE4K-01#show run int gi1/1
Building configuration...

Current configuration : 342 bytes
!
interface GigabitEthernet1/1
 description Connect to IE5K-1 Gig 1/20
 switchport trunk allowed vlan 10,11,18,21,901,918,920
 switchport trunk native vlan 901
 switchport mode trunk
 load-interval 30
```

```
 rep segment 15
 spanning-tree link-type point-to-point
 service-policy input CIP-PTP-Traffic
 service-policy output PTP-Event-Priority
end

IAPTP-IE4K-01#show run int gi1/2
Building configuration...

Current configuration : 348 bytes
!
interface GigabitEthernet1/2
 description Connect to IAPTP-IE4K-02 Gig 1/1
 switchport trunk allowed vlan 10,11,18,21,901,918,920
 switchport trunk native vlan 901
 switchport mode trunk
 load-interval 30
 rep segment 15
 spanning-tree link-type point-to-point
 service-policy input CIP-PTP-Traffic
 service-policy output PTP-Event-Priority
end

IAPTP-IE4K-01#IAPTP-IE4K-01#show ver | inc RELEASE SOFTWARE|Version|image
Cisco IOS Software, IE4000  Software (IE4000-UNIVERSALK9-M), Experimental Version 15.2(20190515:094847)
[vadasser-7_e_rep 113]
BOOTLDR: IE4000  Boot Loader (IE4000-HBOOT-M) Version 15.2(6.2r)E2, RELEASE SOFTWARE
System image file is "sdflash:ie4000-universalk9-mz_backedout_CSCvd47399.SPA"
Version ID                      : V02
Switch Ports Model                    SW Version            SW Image
IAPTP-IE4K-01#
IAPTP-IE4K-01#show ptp port | inc MASTER|SLAVE|PORT
 PTP PORT DATASET: GigabitEthernet1/1
  Port state: SLAVE
 PTP PORT DATASET: GigabitEthernet1/2
  Port state: MASTER
 PTP PORT DATASET: GigabitEthernet1/3
 PTP PORT DATASET: GigabitEthernet1/4
 PTP PORT DATASET: FastEthernet1/5
 PTP PORT DATASET: FastEthernet1/6
 PTP PORT DATASET: FastEthernet1/7
 PTP PORT DATASET: FastEthernet1/8
 PTP PORT DATASET: FastEthernet1/9
 PTP PORT DATASET: FastEthernet1/10
 PTP PORT DATASET: FastEthernet1/11
 PTP PORT DATASET: FastEthernet1/12
 PTP PORT DATASET: FastEthernet1/13
 PTP PORT DATASET: FastEthernet1/14
 PTP PORT DATASET: FastEthernet1/15
 PTP PORT DATASET: FastEthernet1/16
IAPTP-IE4K-01#
IAPTP-IE4K-01#show run int gi1/1
Building configuration...

Current configuration : 342 bytes
!
interface GigabitEthernet1/1
 description Connect to IE5K-1 Gig 1/20
 switchport trunk allowed vlan 10,11,18,21,901,918,920
 switchport trunk native vlan 901
 switchport mode trunk
 load-interval 30
 rep segment 15
```

```
 spanning-tree link-type point-to-point
 service-policy input CIP-PTP-Traffic
 service-policy output PTP-Event-Priority
end

IAPTP-IE4K-01#
IAPTP-IE4K-01#show run int gi1/2
Building configuration...

Current configuration : 348 bytes
!
interface GigabitEthernet1/2
 description Connect to IAPTP-IE4K-02 Gig 1/1
 switchport trunk allowed vlan 10,11,18,21,901,918,920
 switchport trunk native vlan 901
 switchport mode trunk
 load-interval 30
 rep segment 15
 spanning-tree link-type point-to-point
 service-policy input CIP-PTP-Traffic
 service-policy output PTP-Event-Priority
end

IAPTP-IE4K-01#
IAPTP-IE4K-01#show ptp parent
 PTP PARENT PROPERTIES
  Parent Clock:
  Parent Clock Identity: 0xD4:E8:80:FF:FE:6:F2:0
  Parent Port Number: 20
  Observed Parent Offset (log variance): N/A
  Observed Parent Clock Phase Change Rate: N/A

  Grandmaster Clock:
  Grandmaster Clock Identity: 0xEC:46:70:FF:FE:0:24:E4
  Grandmaster Clock Quality:
        Class: 6
        Accuracy: Within 100ns
        Offset (log variance): 13563
        Priority1: 1
        Priority2: 1

IAPTP-IE4K-01#
IAPTP-IE4K-01#show ptp clock
 PTP CLOCK INFO
  PTP Device Type: Boundary clock
  PTP Device Profile: Default Profile
  Clock Identity: 0x70:C9:C6:FF:FE:A8:85:80
  Clock Domain: 0
  Number of PTP ports: 16
  Time Transfer: Feedforward
  Priority1: 110
  Priority2: 111
  Clock Quality:
        Class: 248
        Accuracy: Unknown
        Offset (log variance): N/A
  Offset From Master(ns): -14
  Mean Path Delay(ns): 44
  Steps Removed: 3
  Local clock time: 10:53:39 EDT May 25 2019

IAPTP-IE4K-01#
IAPTP-IE4K-01#show ptp time-property
 PTP CLOCK TIME PROPERTY
  Current UTC offset valid: TRUE
```

```
  Current UTC offset: 37
  Leap 59: FALSE
  Leap 61: FALSE
  Time Traceable: TRUE
  Frequency Traceable: TRUE
  PTP Timescale: TRUE
  Time Source: GNSS
  Time Property Persistence: Infinite

IAPTP-IE4K-01#
IAPTP-IE4K-01#show ptp foreign-master-record
 PTP FOREIGN MASTER RECORDS
 Interface GigabitEthernet1/1
   Foreign master port identity: clock id: 0xD4:E8:80:FF:FE:6:F2:0
   Foreign master port identity: port num: 20
   Number of Announce messages: 4
   Message received port: 1
   Time stamps: 415643932, 415641933
 Interface GigabitEthernet1/2
   Empty
 Interface GigabitEthernet1/3
   Empty
 Interface GigabitEthernet1/4
   Empty
 Interface FastEthernet1/5
   Empty
 Interface FastEthernet1/6
   Empty
 Interface FastEthernet1/7
   Empty
 Interface FastEthernet1/8
   Empty
 Interface FastEthernet1/9
   Empty
 Interface FastEthernet1/10
   Empty
 Interface FastEthernet1/11
   Empty
 Interface FastEthernet1/12
   Empty
 Interface FastEthernet1/13
   Empty
 Interface FastEthernet1/14
   Empty
 Interface FastEthernet1/15
   Empty
 Interface FastEthernet1/16
   Empty
IAPTP-IE4K-01#
```

Configuring Cisco IE 3000

For the Cisco IE 3000 PTP Configuration Guide and Restrictions and Limitations for PTP, refer to Configuring Cisco IE 5000, page 103.

Cisco IE 3000 PTP Default Profile Boundary Clock

Note: The Cisco IE 3000 PTP default profile uses End-to-End Transparent Clock, so no configuration is required.

Cisco IE 3000 PTP Default Profile Boundary Clock Configuration Example

Note: The Cisco IE 3000 PTP default profile uses End-to-End Transparent Clock, so no configuration is required.

Configuring Cisco IE 3400

For the Cisco IE 3400 PTP Configuration Guide and Restrictions and Limitations for PTP, refer to Configuring Cisco IE 5000, page 103.

Cisco IE 3400 PTP Default Profile Boundary Clock

Note: The Cisco IE 3400 PTP default profile uses End-to-End Transparent Clock, so no configuration is required.

Cisco IE 3400 PTP Default Profile Boundary Clock Configuration Example

Note: The Cisco IE 3400 PTP default profile uses End-to-End Transparent Clock, so no configuration is required.

Performance

This section describes the performance characterization results of Cisco products for site-wide precision time. Tests were performed for 24 hours to validate product stability. Table 8 through Table 15 provide the time accuracy values by products.

Table 8 High Precision Site-wide Grandmaster Clock Time Distribution Model–Cisco Catalyst 9300

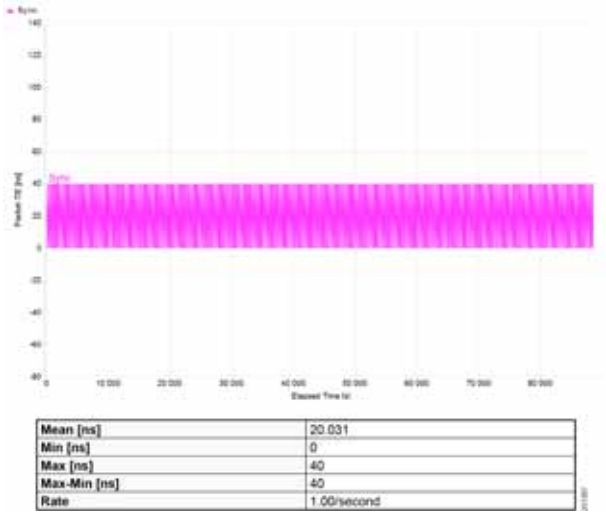
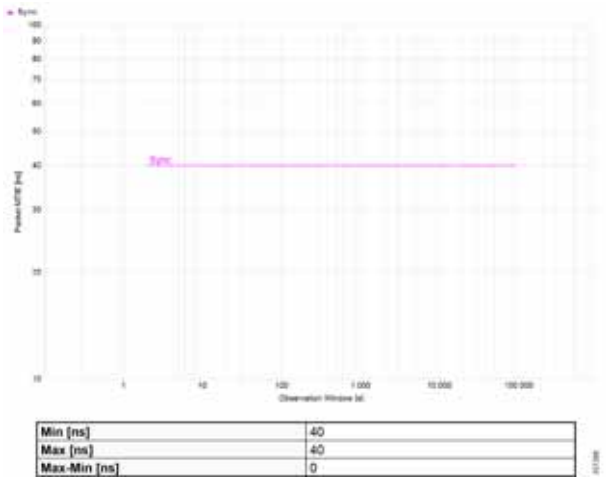
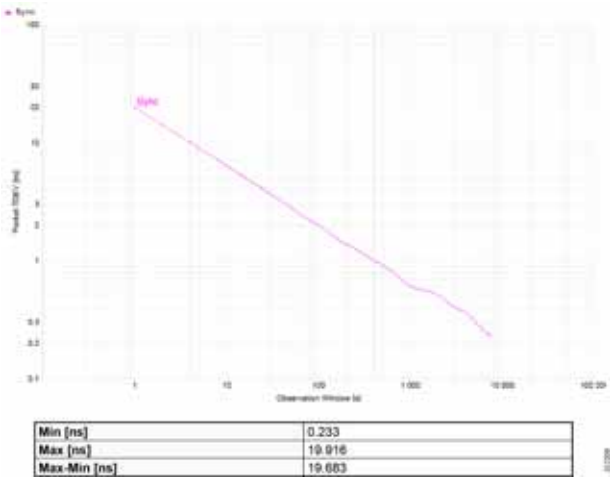
LANTIME M600 Reference	Cisco Catalyst 9300 Boundary Clock	
Time Interval Error (TIE) ±1- 10^{-12}s/24hours	min 40ns max 40ns	 Mean [ns] 20.031 Min [ns] 0 Max [ns] 40 Max-Min [ns] 40 Rate 1.00/second
Maximum Time Interval Error (MTIE) ±1- 10^{-12}s/24hours	min 40ns max 40ns	 Min [ns] 40 Max [ns] 40 Max-Min [ns] 0
Time Deviation (TDEV) NA	min 0.233 max 19.91	 Min [ns] 0.233 Max [ns] 19.916 Max-Min [ns] 19.683

Table 9 High Precision Site-wide Grandmaster Clock Time Distribution Model—Cisco IE 5000

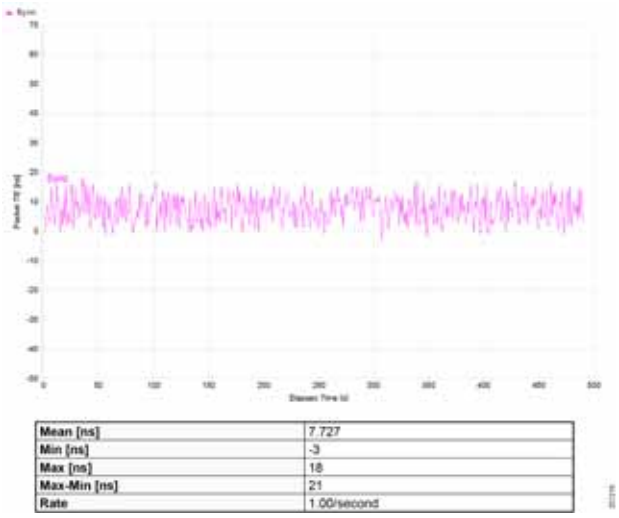
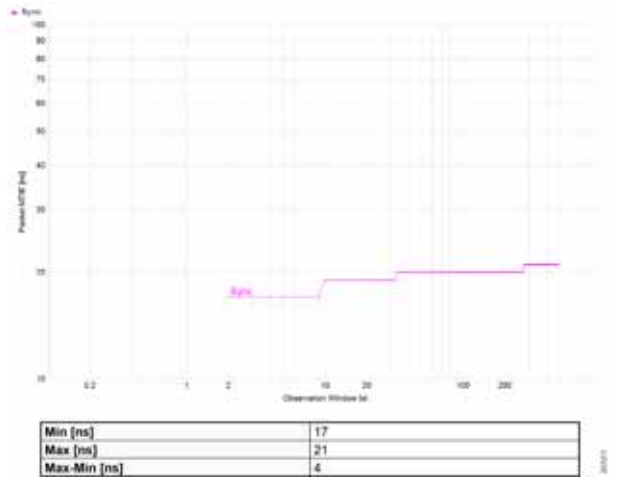
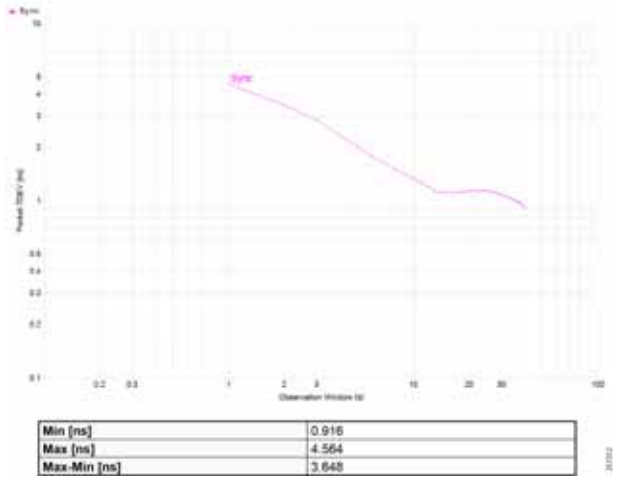
LANTIME M600 Reference	Cisco IE 5000 Boundary Clock	
Time Interval Error (TIE) ±1- 10^{-12}s/24hours	min -3ns max 18ns	 Mean [ns] 7.727 Min [ns] -3 Max [ns] 18 Max-Min [ns] 21 Rate 1.00/second
Maximum Time Interval Error (MTIE) ±1- 10^{-12}s/24hours	min 17ns max 21ns	 Min [ns] 17 Max [ns] 21 Max-Min [ns] 4
Time Deviation (TDEV) NA	min 0.916 max 4.564	 Min [ns] 0.916 Max [ns] 4.564 Max-Min [ns] 3.648

Table 10 High Precision Site-wide Grandmaster Clock Time Distribution Model–Cisco IE 4000

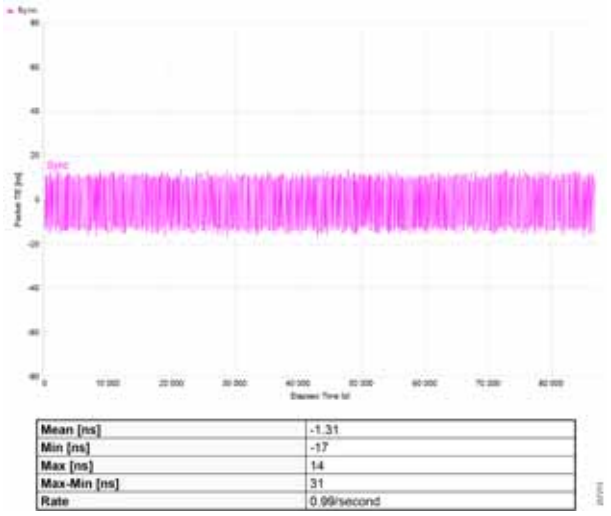
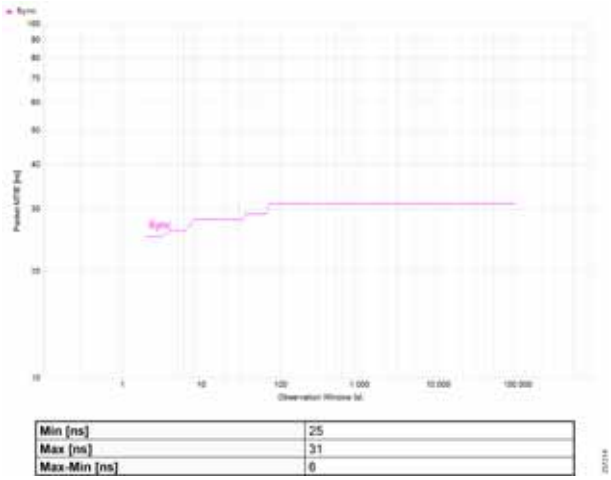
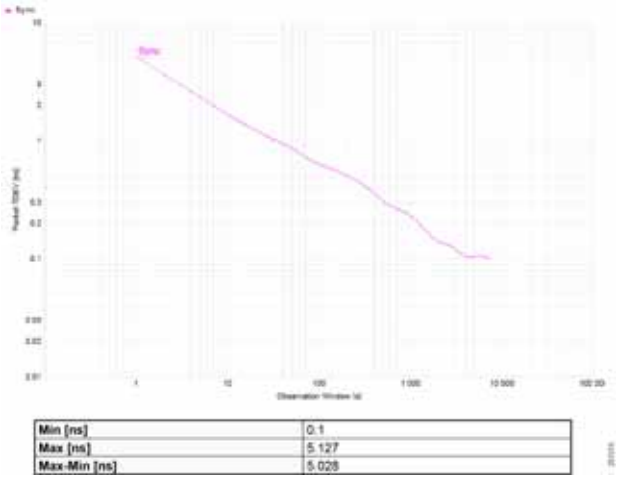
LANTIME M600 Reference	Cisco IE 4000 Boundary Clock and Transparent Clock	
Time Interval Error (TIE) ±1- 10^{-12}s/24hours	min -17ns max 14ns	 Mean [ns] -1.31 Min [ns] -17 Max [ns] 14 Max-Min [ns] 31 Rate 0.99/second
Maximum Time Interval Error (MTIE) ±1- 10^{-12}s/24hours	min 25ns max 31ns	 Min [ns] 25 Max [ns] 31 Max-Min [ns] 6
Time Deviation (TDEV) NA	min 0.1 max 5.127	 Min [ns] 0.1 Max [ns] 5.127 Max-Min [ns] 5.028

Table 11 High Precision Site-wide Grandmaster Clock Time Distribution Model—Cisco IE 3000

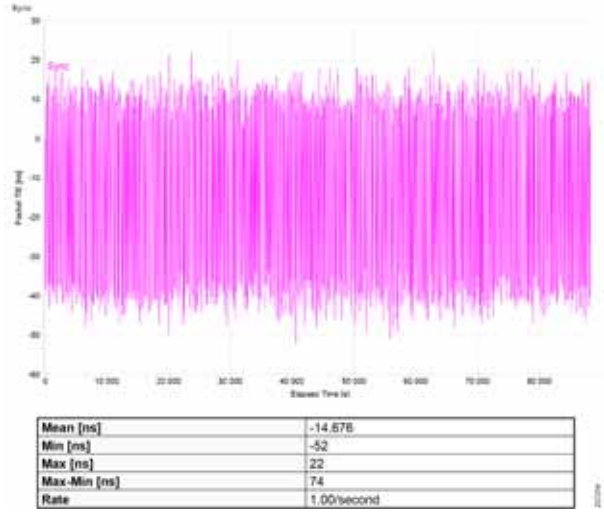
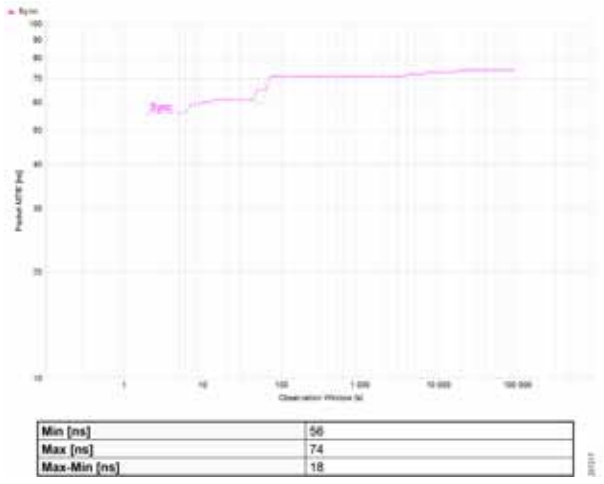
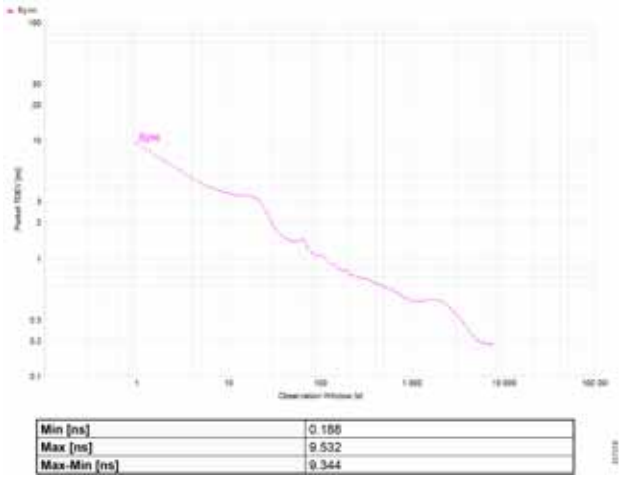
LANTIME M600 Reference	Cisco IE 3000 Transparent Clock	
Time Interval Error (TIE) ±1- 10^{-12}s/24hours	min -52ns max 22ns	
Maximum Time Interval Error (MTIE) ±1- 10^{-12}s/24hours	min 56ns max 74ns	
Time Deviation (TDEV) NA	min 0.188 max 9.532	

Table 12 High Precision Site-wide Grandmaster Clock Time Distribution Model–Cisco IE 3400

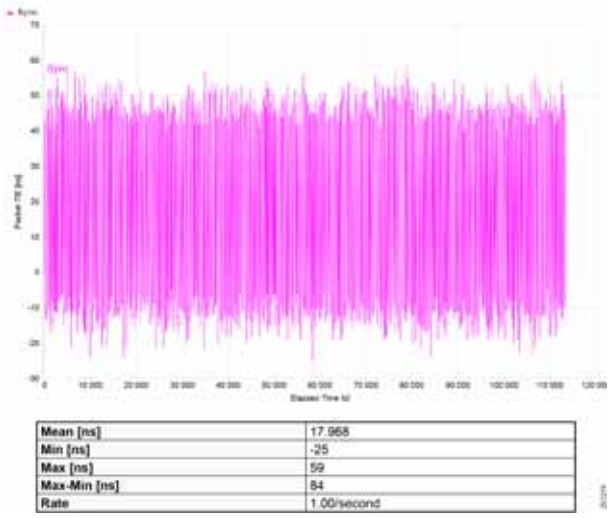
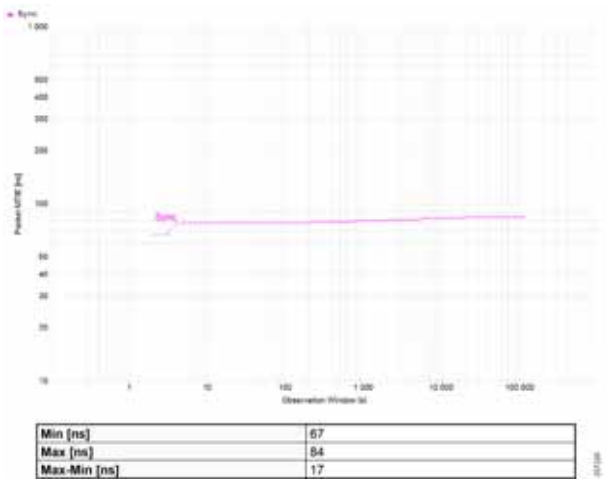
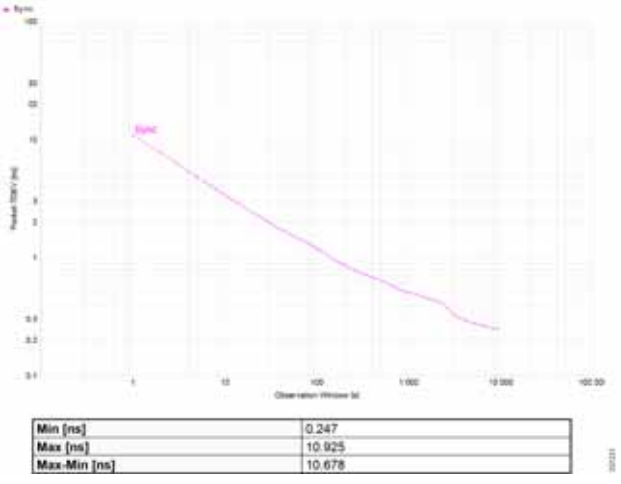
LANTIME M600 Reference	Cisco IE 3400 Transparent Clock	
Time Interval Error (TIE) ±1- 10^{-12}s/24hours	min -25ns max 59ns	 Mean [ns] 17.968 Min [ns] -25 Max [ns] 59 Max-Min [ns] 84 Rate 1.00/second
Maximum Time Interval Error (MTIE) ±1- 10^{-12}s/24hours	min 67ns max 84ns	 Min [ns] 67 Max [ns] 84 Max-Min [ns] 17
Time Deviation (TDEV) NA	min 0.247ns max 10.925ns	 Min [ns] 0.247 Max [ns] 10.925 Max-Min [ns] 10.678

Table 13 Intermediate Precision Site-wide Grandmaster Clock Time Distribution Model—Cisco IE 4000

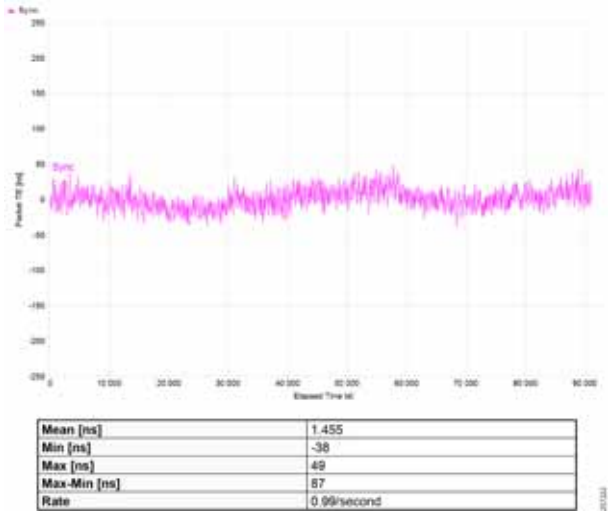
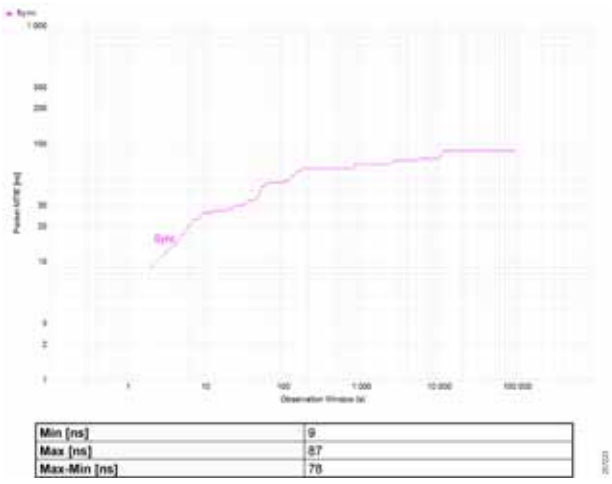
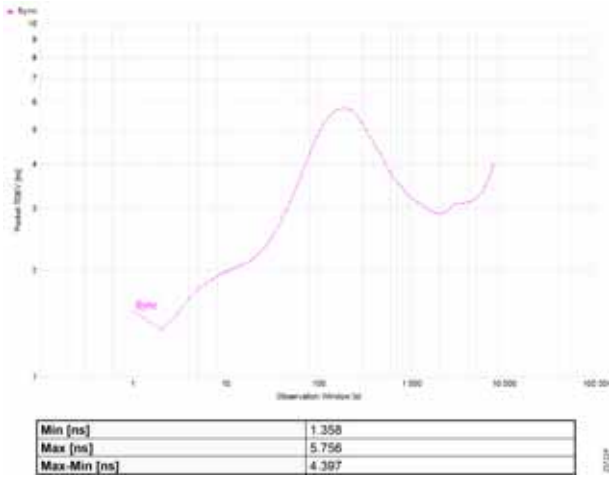
Cisco IE 5000 Reference	Cisco IE 4000 Boundary Clock and Transparent Clock	
Time Interval Error (TIE) ±4.6-6 s/17hours	min -38ns max 49ns	 Mean [ns] 1.455 Min [ns] -38 Max [ns] 49 Max-Min [ns] 87 Rate 0.99/second
Maximum Time Interval Error (MTIE) ±4.6-6 s/17hours	min 9ns max 87ns	 Min [ns] 9 Max [ns] 87 Max-Min [ns] 78
Time Deviation (TDEV) NA	min 1.358 max 5.756	 Min [ns] 1.358 Max [ns] 5.756 Max-Min [ns] 4.397

Table 14 Intermediate Precision Site-wide Grandmaster Clock Time Distribution Model—Cisco IE 3000

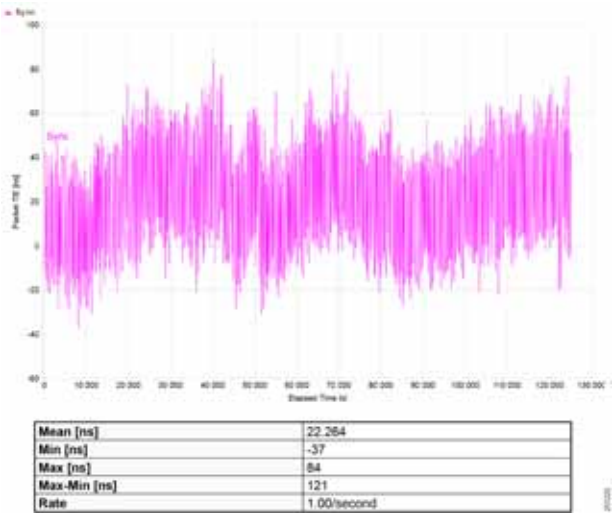
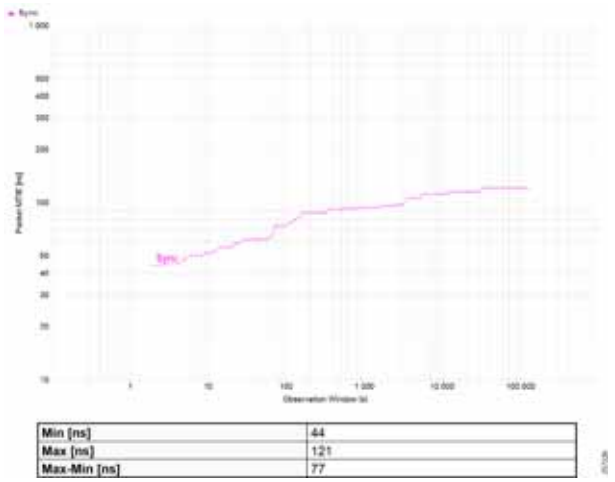
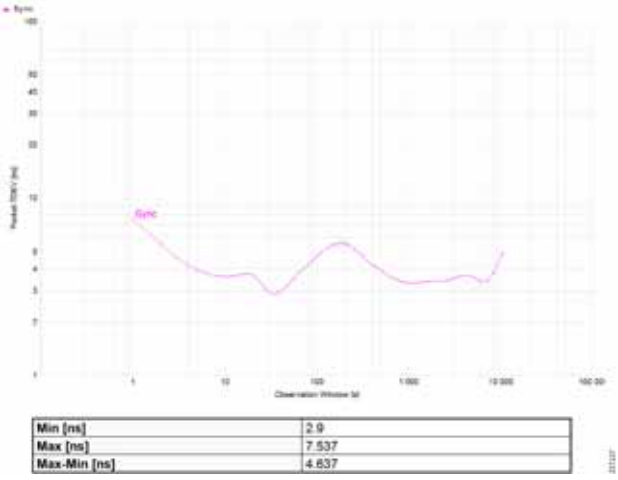
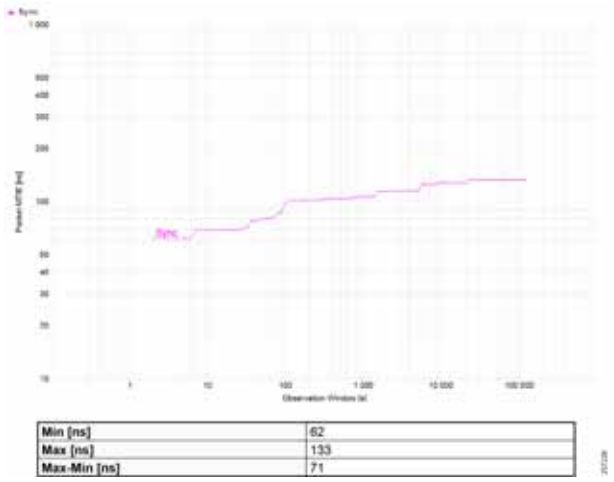
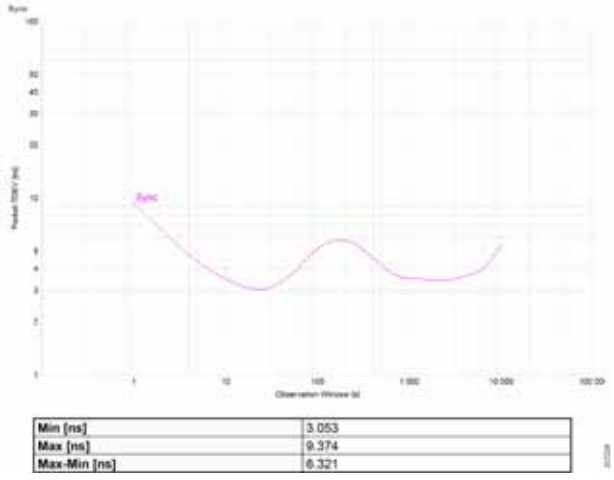
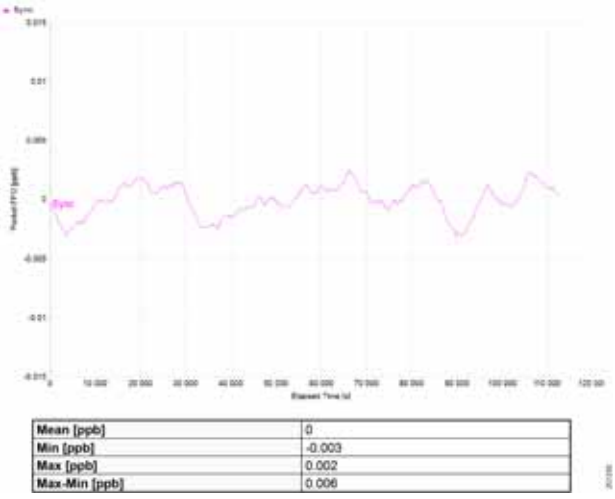
Cisco IE 5000 Reference	Cisco IE 3000 Transparent Clock	
Time Interval Error (TIE) ±4.6-6 s/17hours	min -37ns max 84ns	 Mean [ns] 22.264 Min [ns] -37 Max [ns] 84 Max-Min [ns] 121 Rate 1.00/second
Maximum Time Interval Error (MTIE) ±4.6-6 s/17hours	min 44ns max 121ns	 Min [ns] 44 Max [ns] 121 Max-Min [ns] 77
Time Deviation (TDEV) NA	min 2.9 max 7.537	 Min [ns] 2.9 Max [ns] 7.537 Max-Min [ns] 4.637

Table 15 Intermediate Precision Site-wide Grandmaster Clock Time Distribution Model—Cisco IE 3400

Cisco IE 5000 Reference	Cisco IE 3400 Transparent Clock	
Time Interval Error (TIE) ±4.6-6 s/17hours	min -98ns max 35ns	
Maximum Time Interval Error (MTIE) ±4.6-6 s/17hours	min 62ns max 133ns	
Time Deviation (TDEV) NA	min 3.053 max 9.374	

Troubleshooting the Infrastructure

This section includes the following major topics:

TrustSec Troubleshooting Tips on Cisco Switches

The following section describes certain show commands that can be executed to view potential sources of problems related to Cisco TrustSec.

Note: An IT engineer should have some expertise in TrustSec in order to troubleshoot any problems that are discovered. For complete information on Cisco TrustSec troubleshooting tips, refer to the following URL: https://community.cisco.com/t5/security-documents/trustsec-troubleshooting-guide/ta-p/3647576

Cisco IE Switch is Unable to Register with Cisco ISE and Download the SGT Table Information

Verify TrustSec Credentials

This is the first step and it is possible that the IT security administrator might missed or entered incorrect TrustSec credentials on the switch or in ISE. Issue the following command:

```
IE4K-25#show cts credentials
CTS password is defined in keystore, device-id = IE4K-25
```

Verify the PAC Key

The PAC key must match between the Cisco ISE and the switch. If there is a mismatch, you must re-configure the key, which will force a new PAC provisioning in the switch. To verify the PAC is installed:

```
IE4K-25#show cts pacs
  AID: BA6AAD6CB6C10E7045A4CCD0DA18E706
  PAC-Info:
    PAC-type = Cisco Trustsec
    AID: BA6AAD6CB6C10E7045A4CCD0DA18E706
    I-ID: IE4K-25
    A-ID-Info: Identity Services Engine
    Credential Lifetime: 12:45:25 EST Nov 10 2018
  PAC-Opaque:
000200B000030001000400010BA6AAD6CB6C10E7045A4CCD0DA18E706000060094000301000AA913A603C53109269B2EACF49C
2DED3000000135B68B9AB00093A804EB1C0FC8CF53471B62A122C4BB434A3BE2D7C13B59FA9D3BA8DF17CB7988B1E8BE785
6DDC50C4F5CA6B20FE8E78270AB163FA73897FAFD7010325AEB3D8CD208D92A1B7BBD2C483D01CA4EE6B8FB9B7AFBF9CA8A
5AE2274ECDE5BB9C457674376A48865BADF98C43B2CFC9FA8B8D3FD72FC538B
  Refresh timer is set for 8w4d

IE4K-25#
```

To clear the credentials:

```
clear cts credentials
clear cts pac
```

Verify that RADIUS is Operational from the Switch

```
IE4K-25#show aaa servers
```

```
RADIUS: id 1, priority 1, host 10.13.48.184, auth-port 1812, acct-port 1813
     State: current UP, duration 2488903s, previous duration 0s
     Dead: total time 0s, count 5968
     Quarantined: No
     Authen: request 2275, timeouts 0, failover 0, retransmission 0
             Response: accept 20, reject 2255, challenge 0
             Response: unexpected 0, server error 0, incorrect 0, time 32ms
             Transaction: success 2275, failure 0
             Throttled: transaction 0, timeout 0, failure 0
     Author: request 2, timeouts 0, failover 0, retransmission 0
             Response: accept 2, reject 0, challenge 0
             Response: unexpected 0, server error 0, incorrect 0, time 50ms
             Transaction: success 2, failure 0
             Throttled: transaction 0, timeout 0, failure 0
     Account: request 38, timeouts 0, failover 0, retransmission 0
             Request: start 18, interim 0, stop 18
             Response: start 18, interim 0, stop 18
             Response: unexpected 0, server error 0, incorrect 0, time 29ms
             Transaction: success 38, failure 0
             Throttled: transaction 0, timeout 0, failure 0
     Elapsed time since counters last cleared: 4w19h26m
     Estimated Outstanding Access Transactions: 0
     Estimated Outstanding Accounting Transactions: 0
     Estimated Throttled Access Transactions: 0
     Estimated Throttled Accounting Transactions: 0
     Maximum Throttled Transactions: access 0, accounting 0
     Requests per minute past 24 hours:
             high - 15 hours, 42 minutes ago: 2
             low  - 0 hours, 0 minutes ago: 0
             average: 0
IE4K-25#
```

Verify the CTS Server Configuration

The command to verify the cts server-list is shown below:

```
IE4K-25#show cts server-list
CTS Server Radius Load Balance = DISABLED
Server Group Deadtime = 20 secs (default)
Global Server Liveness Automated Test Deadtime = 20 secs
Global Server Liveness Automated Test Idle Time = 60 mins
Global Server Liveness Automated Test = DISABLED

Installed list: CTSServerList1-000B, 1 server(s):
 *Server: 10.13.48.184, port 1812, A-ID 75FD68D130DA33A44480ED005C93FF49
          Status = ALIVE
          auto-test = FALSE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
IE4K-25#
```

Verify the Downloaded SGT Mappings

```
IE4K-25#show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
  SGT tag = 0-00:Unknown
Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
 *Server: 10.13.48.184, port 1812, A-ID BA6AAD6CB6C10E7045A4CCD0DA18E706
          Status = ALIVE
          auto-test = FALSE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
```

```
Multicast Group SGT Table:
Security Group Name Table:
    0-fd:Unknown
    2-fd:TrustSec_Devices
    3-fd:LEVEL_1_GENERIC
    4-fd:LEVEL_1_GENERIC_IO
    5-fd:LEVEL_0_IO
    6-fd:LEVEL_3
    7-fd:LEVEL_1_CONTROLLER
    8-fd:Remote_Access
    10-fd:Remote_Desktop
    255-fd:Quarantined_Systems
Environment Data Lifetime = 86400 secs
Last update time = 10:18:52 EDT Sun Sep 9 2018
Env-data expires in   0:01:08:23 (dd:hr:mm:sec)
Env-data refreshes in 0:01:08:23 (dd:hr:mm:sec)
Cache data applied           = NONE
State Machine is running
IE4K-25#
```

IACS Asset is Unable to Authenticate to Cisco ISE

This section describes how to troubleshoot when an IACS device is unable to authenticate to Cisco ISE.

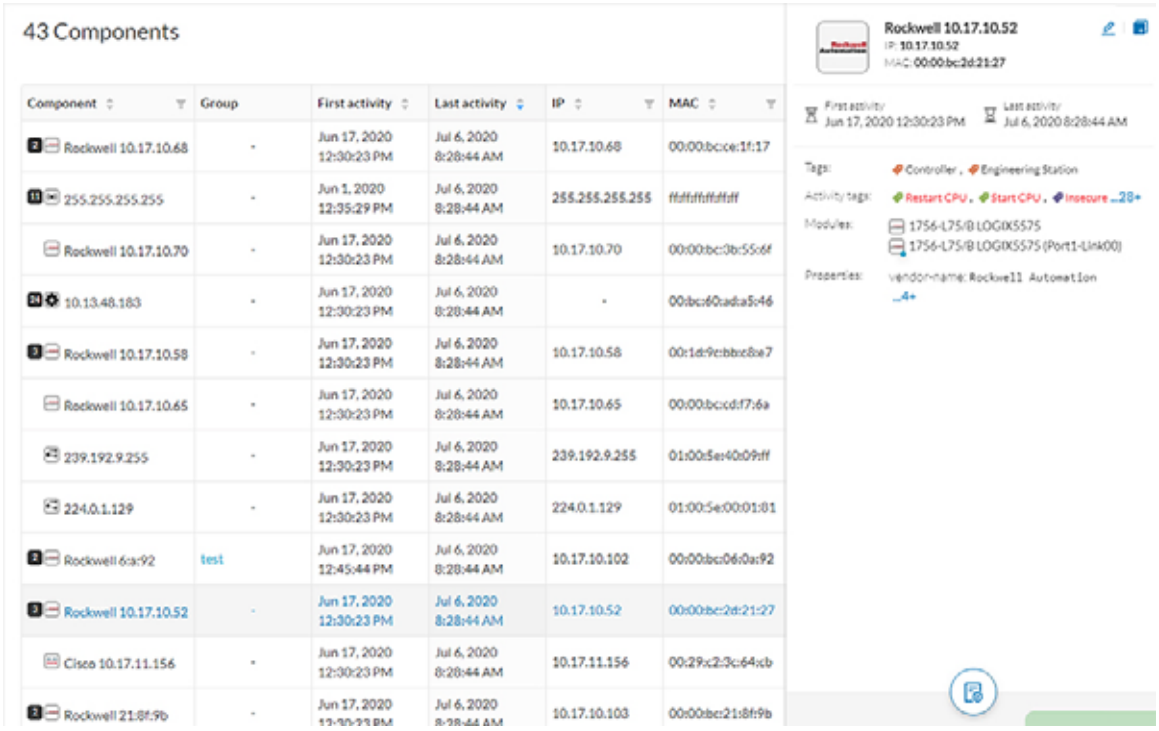
Verify the Authentication and Authorization State of IACS Assets on the Switch

```
IE4K-34# show authentication brief

Interface  MAC Address     AuthC           AuthZ                    Fg  Uptime
-----------------------------------------------------------------------------
Gi1/14     0000.bc3f.d0ef  m:OK            AZ: SA-                      409219s
Gi1/16     0000.bccd.f76a  m:OK            AZ: SA-                      409221s
Gi1/11     0000.bc2d.20ef  m:CF            UZ: SA- FA-                  409221s

Session count = 3

Key to Authentication Attributes:

 RN - Running
 ST - Stopped
 OK - Authentication Success
 CF - Credential Failure
 AD - AAA Server Failure
 NR - No Response
 TO - Timeout
 AR - AAA Not Ready

Key to Authorization Attributes:

 AZ - Authorized, UZ - UnAuthorized
 SA - Success Attributes, FA - Failed Attributes
 D: - DACL, F: - Filterid / InACL, U: - URL ACL
 V: - Vlan, I: - Inactivity Timer, O: - Open Dir

Key to Session Events Blocked Status Flags:

  A - Applying Policy (multi-line status for details)
  D - Awaiting Deletion
  F - Final Removal in progress
  I - Awaiting IIF ID allocation
  N - Waiting for AAA to come up
  P - Pushed Session
  R - Removing User Profile (multi-line status for details)
  U - Applying User Profile (multi-line status for details)
```

```
  X - Unknown Blocker
IE4K-34#
```

Verify Cisco Cyber Vision has Discovered the IACS Asset

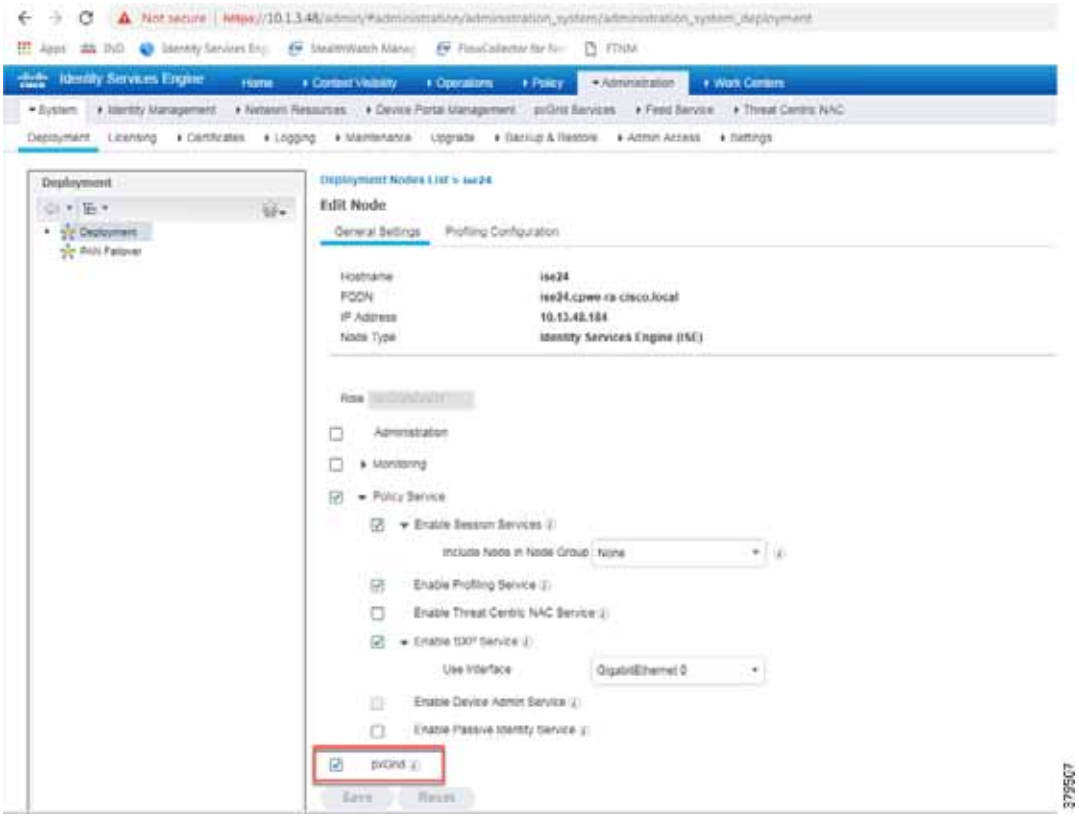
Figure 50 Cisco Cyber Vision Discovering IACS Asset



Verify the pxGrid Service is Enabled on Cisco ISE

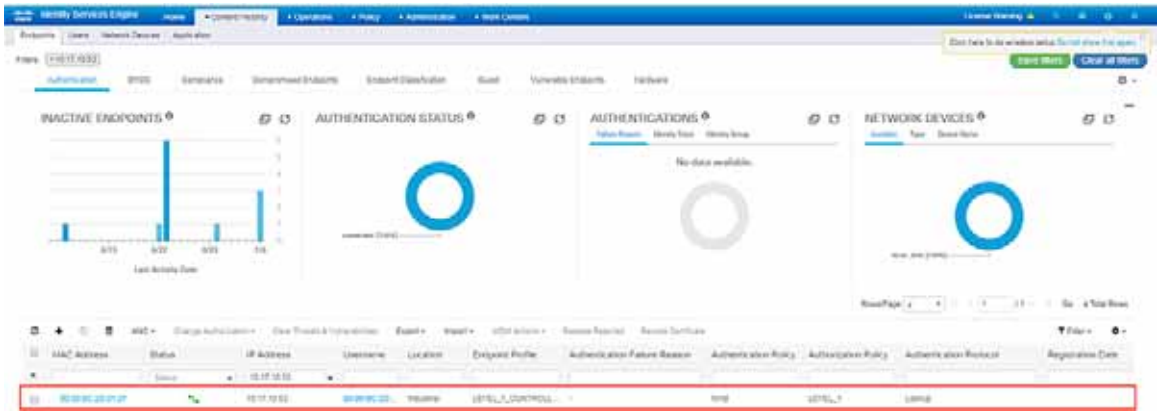
From the Cisco ISE web UI, navigate to **Administration -> Deployment**. Check the checkbox of the appropriate PSN and click **Edit**. Verify the **pxGrid** check box is checked.

Figure 51 Verifying that the pxGrid Service is Enabled at Cisco ISE



The next step is to verify if Cisco ISE has the IACS asset in the endpoint database.

Figure 52 Cisco ISE has Learned the IACS Asset



Verify that Profiling Policies are Configured Correctly

ISE profiles the IACS assets based on the profiling policy. If conditions in the profiling policy are not configured correctly, then ISE will not be able to profile the IACS asset.

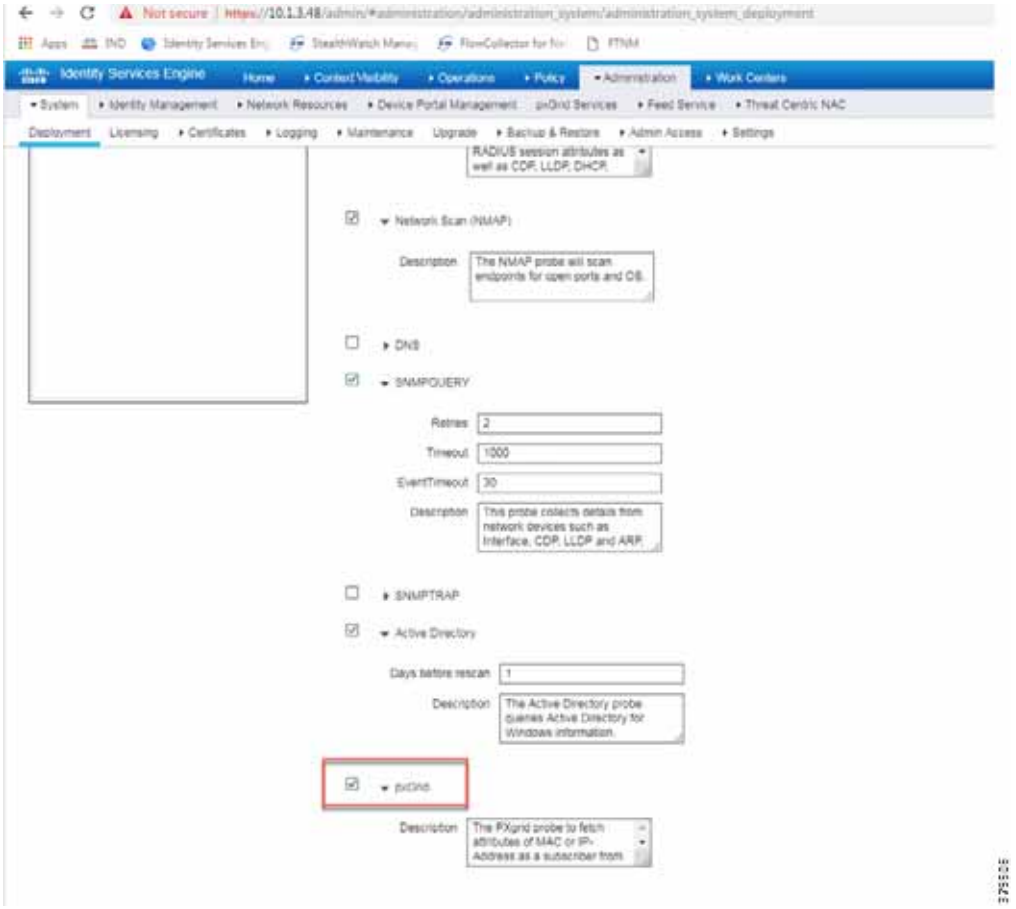
Verify that Authentication and Authorization Policies are Configured Correctly in Cisco ISE

To assign an SGT to an IACS asset, the authentication and authorization policy conditions must match to the IACS device attributes.

Verify the pxGrid Probe is Enabled on the PSN

From the Cisco ISE web UI, navigate to **Administration -> Deployment**. Check the checkbox of the appropriate PSN and click **Edit**. Click the **Profiling Configuration** tab, then verify the **pxGrid** check box is checked

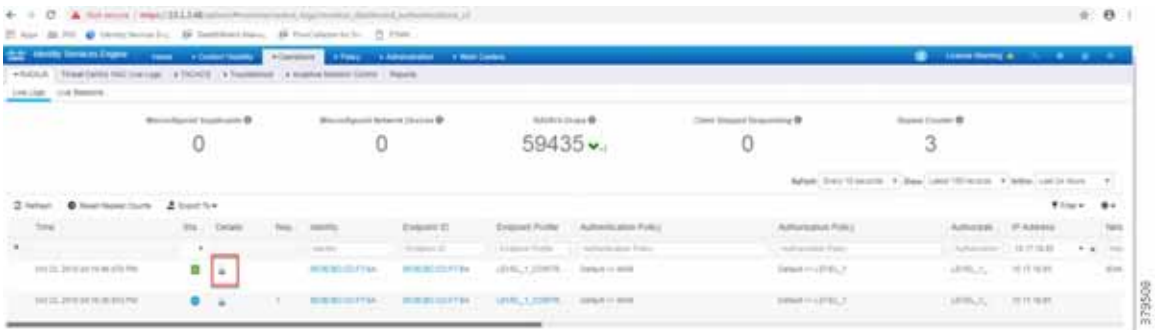
Figure 53 Verifying that pxGrid Probe is Enabled on the PSN



Verify Authentication and Authorization from RADIUS Live Logs

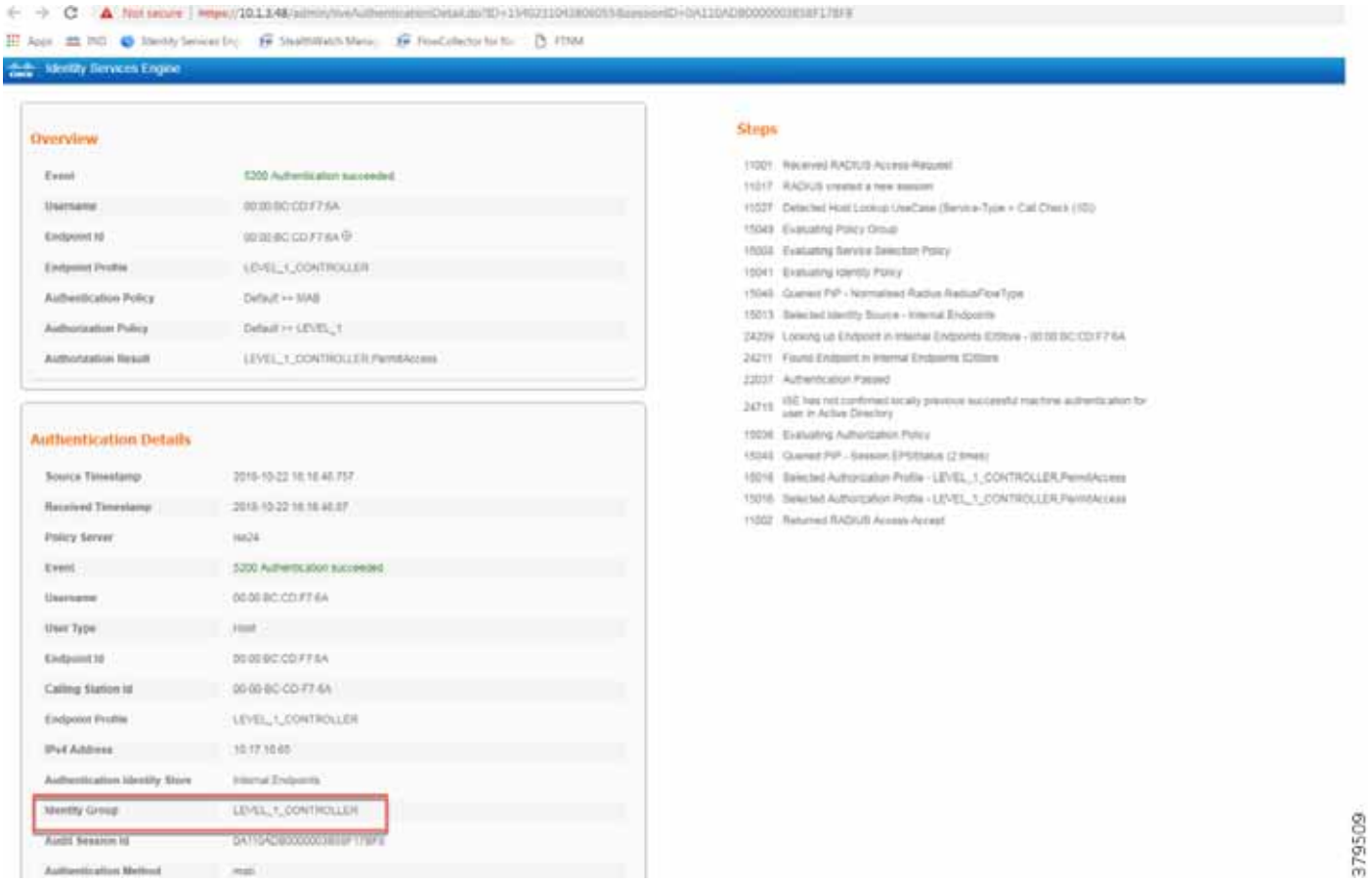
From the ISE web UI, navigate to **Operations -> RADIUS -> Live Logs** to view a list of devices that went through the authentication and authorization process.

Figure 54 Live Logs at ISE



Click the icon in the Details column to view information about the asset and the RADIUS process.

Figure 55 Authentication and Authorization Results of an IACS Asset



Distribution Switch is not Enforcing the Policy Correctly

Verify the SGT Assignment

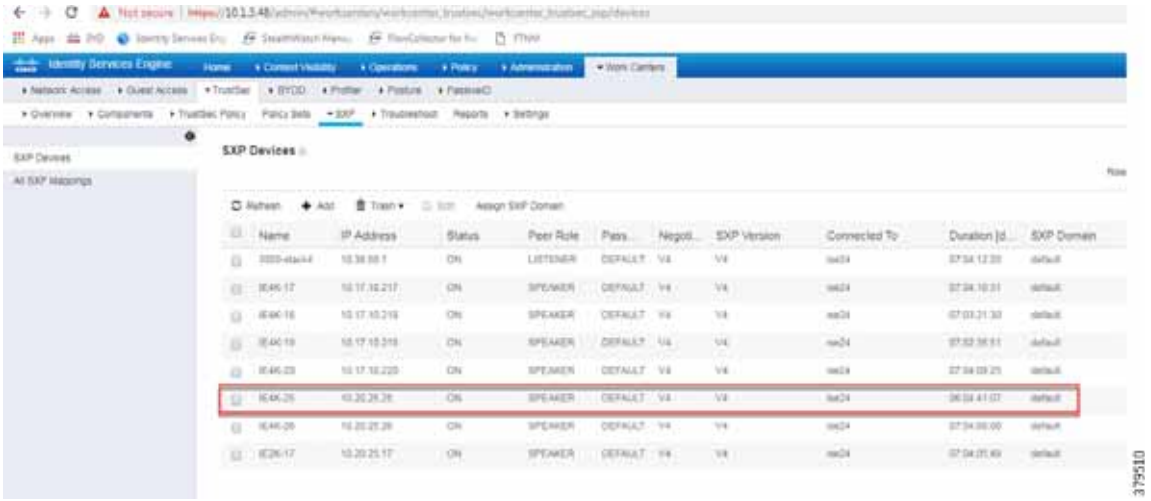
```
IE4K-25#show cts role-based sgt-map all
Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
10.13.15.25             4       INTERNAL
10.20.25.12             11      LOCAL
10.20.25.25             4       INTERNAL
10.20.25.221            5       LOCAL
10.20.26.25             4       INTERNAL
10.20.50.5              4       INTERNAL
192.168.4.25            4       INTERNAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 2
Total number of INTERNAL bindings = 5
Total number of active   bindings = 7

IE4K-25#
```

Verify the SXP Connection between the Cisco ISE and the Switch

```
IE4K-25#show cts sxp connections
 SXP              : Enabled
 Highest Version Supported: 4
 Default Password : Set
 Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is not running
Peer-Sequence traverse limit for export: Not Set
Peer-Sequence traverse limit for import: Not Set
----------------------------------------------
Peer IP           : 10.13.48.184
Source IP         : 10.20.25.25
Conn status       : On
Conn version      : 4
Conn capability   : IPv4-IPv6-Subnet
Conn hold time    : 120 seconds
Local mode        : SXP Speaker
Connection inst#  : 1
TCP conn fd       : 1
TCP conn password: default SXP password
Keepalive timer is running
Duration since last state change: 6:01:28:42 (dd:hr:mm:sec)


Total num of SXP Connections = 1
```

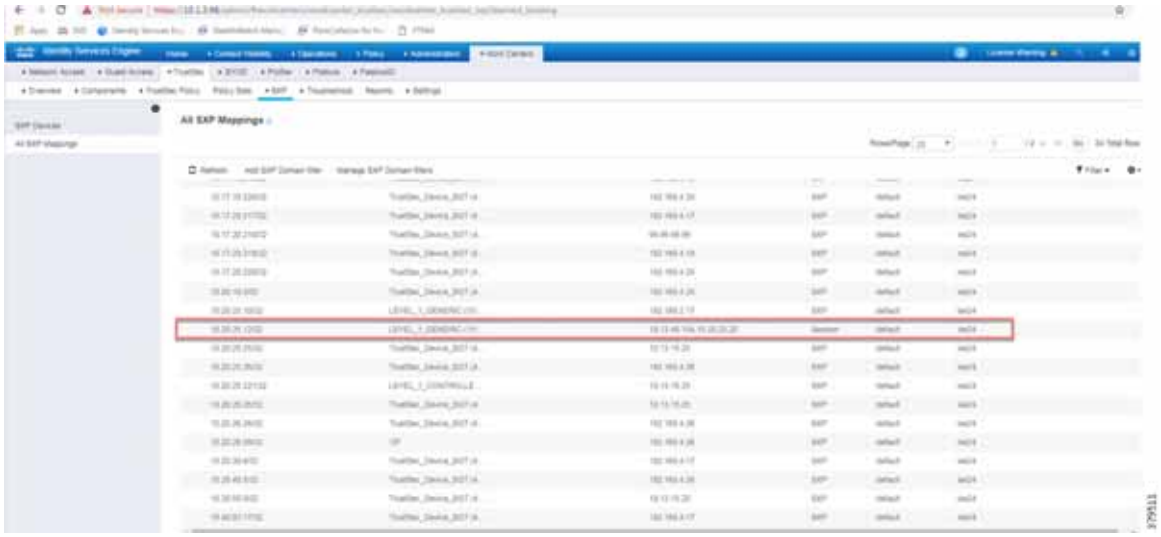
In addition, from the Cisco ISE web UI, navigate to **Work Centers -> TrustSec -> SXP** and verify the SXP status.

Figure 56 Verifying the SXP Status in ISE



Verify Cisco ISE has Received the SGT-IP Mapping Information through the SXP Tunnel

Figure 57 Verifying the SXP Status of a Switch at ISE



Verify the Distribution Switch has Received SGT Mappings through SXP

```
P5-9300-2#sho cts sxp sgt-map brief
SXP Node ID(generated):0xC0A80A2A(192.168.10.42)
IP-SGT Mappings as follows:
IPv4,SGT: <10.17.10.52 , 5:LEVEL_1_CONTROLLER>
IPv4,SGT: <10.17.10.70 , 8:LEVEL_3>
IPv4,SGT: <10.17.15.128 , 8:LEVEL_3>
IPv4,SGT: <10.17.25.79 , 5:LEVEL_1_CONTROLLER>
IPv4,SGT: <10.17.25.129 , 11:LEVEL_1_GENERIC>
```

Verify that Policy Matrix is Downloaded to the Distribution Switch

```
P5-9300-2#show cts role-based permissions
IPv4 Role-based permissions from group 5:LEVEL_1_CONTROLLER to group 5:LEVEL_1_CONTROLLER:
    Deny IP-00
IPv4 Role-based permissions from group 6:LEVEL_0_IO to group 5:LEVEL_1_CONTROLLER:
    Deny IP-00
IPv4 Role-based permissions from group 8:LEVEL_3 to group 5:LEVEL_1_CONTROLLER:
    Permit IP-00
IPv4 Role-based permissions from group 9:Remote_Access to group 5:LEVEL_1_CONTROLLER:
    Deny IP-00
IPv4 Role-based permissions from group 10:Remote_Desktop to group 5:LEVEL_1_CONTROLLER:
    Deny IP-00
IPv4 Role-based permissions from group 5:LEVEL_1_CONTROLLER to group 6:LEVEL_0_IO:
    Deny IP-00
IPv4 Role-based permissions from group 6:LEVEL_0_IO to group 6:LEVEL_0_IO:
    Deny IP-00
IPv4 Role-based permissions from group 8:LEVEL_3 to group 6:LEVEL_0_IO:
    Permit IP-00
IPv4 Role-based permissions from group 9:Remote_Access to group 6:LEVEL_0_IO:
    Deny IP-00
IPv4 Role-based permissions from group 10:Remote_Desktop to group 6:LEVEL_0_IO:
    Deny IP-00
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

Cisco ISE Troubleshooting Tips

The following section provides high level troubleshooting information to assist in identifying and resolving problems you may encounter when you use the Cisco ISE.

Note: For complete information on Cisco ISE monitoring and troubleshooting tips, refer to the following URL: https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ise_admin_guide_24/b_ise_admin_guide_24_new_chapter_011001.html

Checking the Status of pxGrid

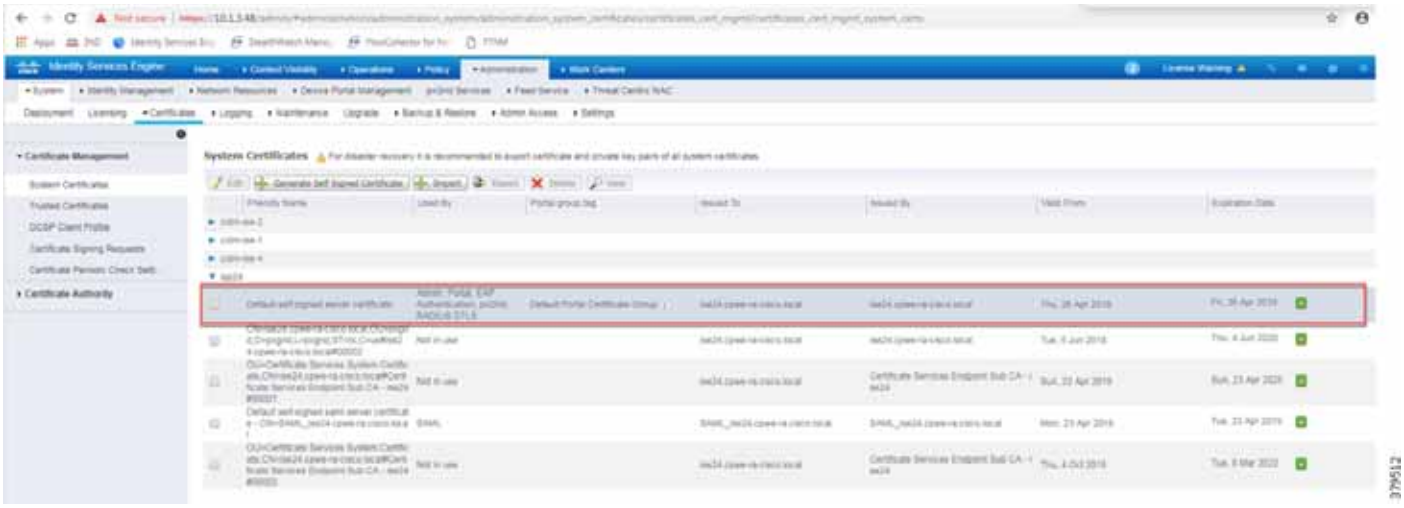
On the PSN, execute the following command to check the status of the pxGrid:

```
ise24/admin# show application status ise | include pxGrid
pxGrid Infrastructure Service          running          5736
pxGrid Publisher Subscriber Service    running          5880
pxGrid Connection Manager              running          5851
pxGrid Controller                      running          5902
ise24/admin#
```

Verify the pxGrid Certificate on the PSN

From the ISE web UI, navigate to **Administration -> System -> Certificates**. Click the **arrow** button of the PSN to expand its certificate details.

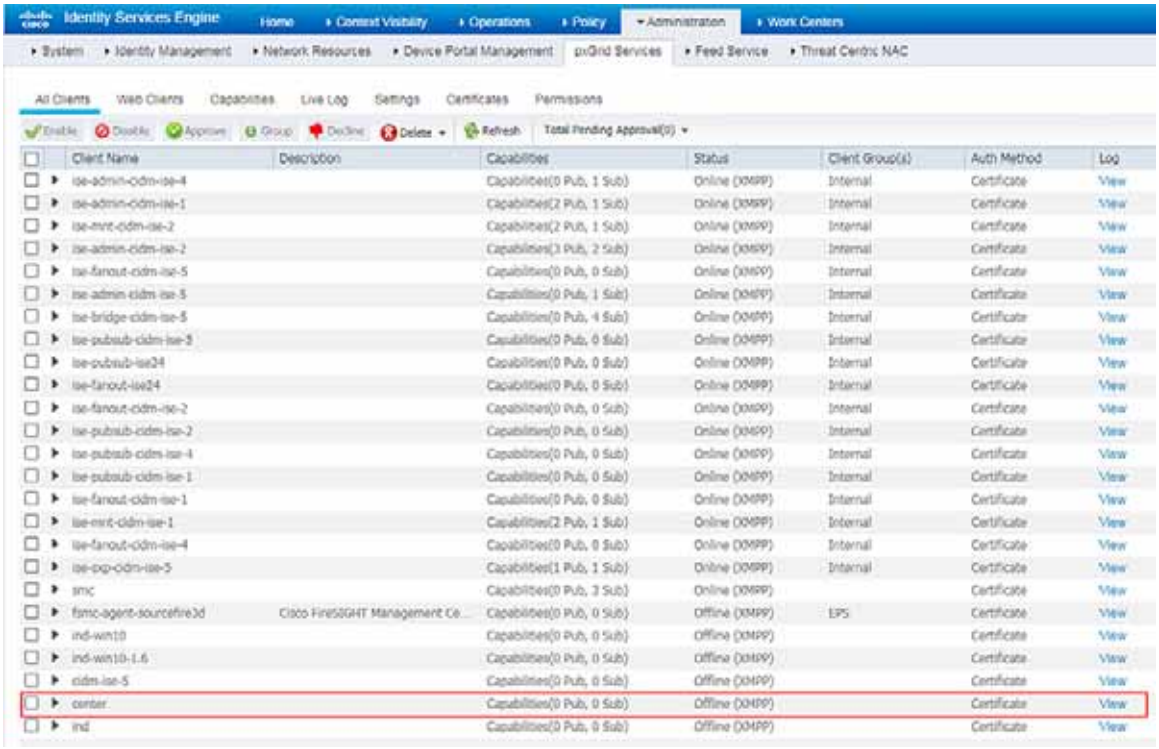
Figure 58 Verifying pxGrid Certificate on the PSN



Verify pxGrid Client Status

From the ISE web UI, navigate to **Administration -> pxGrid Services**. Verify Cisco Cyber Vision is registered as client.

Figure 59 Verifying pxGrid Client Status



Cisco NetFlow Troubleshooting Tips

This section discusses some useful **show** commands for troubleshooting NetFlow records and their transmission.

Verify the NetFlow Record Parameters

```
IE4K-25#show flow record
flow record StealthWatch_Record:
  Description:        NetFlow record format to send to StealthWatch
  No. of users:       1
  Total field space:  59 bytes
  Fields:
    match datalink mac source address input
    match datalink mac destination address input
    match ipv4 tos
    match ipv4 protocol
    match ipv4 source address
    match ipv4 destination address
    match transport source-port
    match transport destination-port
    collect transport tcp flags
    collect interface input
    collect interface output
    collect counter bytes long
    collect counter packets long
    collect timestamp sys-uptime first
    collect timestamp sys-uptime last

IE4K-25#
```

Verify the Flow Exporter Destination IP Address

```
IE4K-25#show flow exporter
Flow Exporter StealthWatch_Exporter:
  Description:              StealthWatch Flow Exporter
  Export protocol:          NetFlow Version 9
  Transport Configuration:
    Destination IP address: 10.13.48.183
    Source IP address:      10.20.50.5
    Transport Protocol:     UDP
    Destination Port:       2055
    Source Port:            52254
    DSCP:                   0x0
    TTL:                    255
    Output Features:        Used
  Options Configuration:
    application-table (timeout 600 seconds)
```

Verify the Flow Monitor Configuration

```
IE4K-25#show flow monitor
Flow Monitor StealthWatch_Monitor:
  Description:       StealthWatch Flow Monitor
  Flow Record:       StealthWatch_Record
  Flow Exporter:     StealthWatch_Exporter
  Cache:
    Type:                 normal
    Status:               allocated
    Size:                 16640 entries / 1529948 bytes
    Inactive Timeout:     30 secs
    Active Timeout:       30 secs
    Update Timeout:       1800 secs
    Synchronized Timeout: 600 secs
```

Verify the Flow Monitor is Applied to an Appropriate Interface

```
IE4K-25#show flow interface gigabitEthernet 1/10
Interface GigabitEthernet1/10
  FNF:  monitor:          StealthWatch_Monitor
        direction:        Input
        traffic(ip):      on
```

Verify the Flow Monitor Cache

```
P5-9300-2#show flow monitor StealthWatch_Monitor cache
  Cache type:                                Normal (Platform cache)
  Cache size:                               Unknown
  Current entries:                                3

  Flows added:                                412595
  Flows aged:                                 412592
    - Active timeout      (    60 secs)     184742
    - Inactive timeout    (    15 secs)     227850

DATALINK MAC SOURCE ADDRESS INPUT:       E865.49DF.7E41
DATALINK MAC DESTINATION ADDRESS INPUT:  0100.5E00.000A
IPV4 SOURCE ADDRESS:                     10.255.255.51
IPV4 DESTINATION ADDRESS:                224.0.0.10
TRNS SOURCE PORT:                        0
TRNS DESTINATION PORT:                   0
IP TOS:                                  0xC0
IP PROTOCOL:                             88
tcp flags:                               0x00
interface output:                        Null
counter bytes long:                      480
```

```
counter packets long:                    8
```

Troubleshooting Cisco Cyber Vision

Cisco Cyber Vision Center and ISE pxGrid Communication

To view the live logs of the pxGrid agent running on the Cisco Cyber Vision Center, do the following:

1. Connect to the Cisco Cyber Vision Center over SSH.
2. Run the following command:

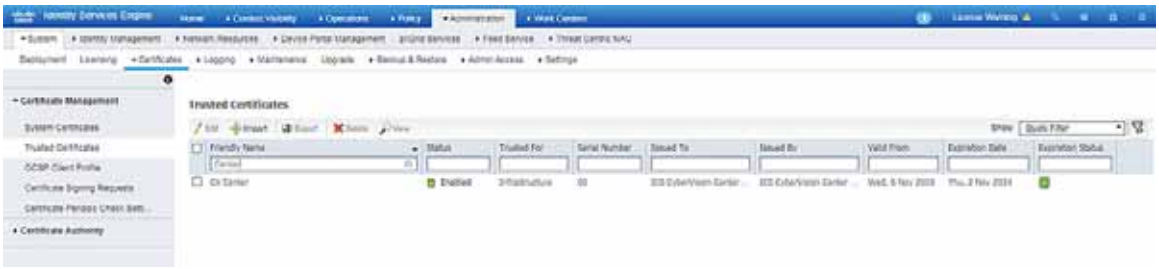
```
Center# journalctl -u pxgrid-agent -f
```

3. The scrolling output will display connection details and data attributes sent to pxGrid. An example of a successful connection:

```
May 28 15:00:55 center pxgrid-agent-start.sh[1374]: pxgrid-agent Websocket connect
url=wss://cidm-ise-5.cpwe-ra-cisco.local:8910/pxgrid/ise/pubsub [caller=endpoint.go:102]
May 28 15:00:55 center pxgrid-agent-start.sh[1374]: pxgrid-agent STOMP CONNECT host=10.13.48.184
[caller=endpoint.go:111]
```

Things to check if the pxGrid connection is not successful:

- The Cisco Cyber Vision Center can successfully ping both the IP address and the FQDN of the ISE pxGrid node.
- The Cisco Cyber Vision Center certificate is in the ISE Trusted Certificates list.



- The Cisco Cyber Vision Center pxGrid certificate was configured correctly (see Cisco ISE Troubleshooting Tips).

ISE Profiling with Cisco Cyber Vision Attributes

To view the attributes being sent from Cisco Cyber Vision, run the following command on the Cisco Cyber Vision Center CLI:

```
Center# journalctl -u pxgrid-agent -f
```

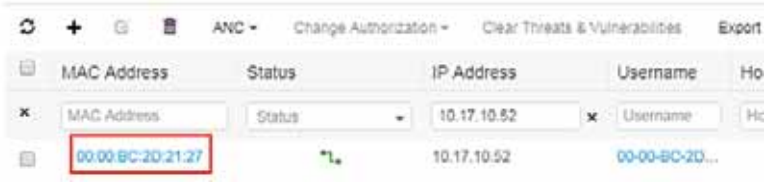
An example of component attributes:

```
Jun 05 15:25:29 center pxgrid-agent-start.sh[1505]: pxgrid-agent STOMP SEND
destination=/topic/com.cisco.endpoint.asset
body={"opType":"UPDATE","asset":{"assetId":"1e276520-7972-5ea1-9467-08a13af01b18,d52e4e10-4da5-5998-b01
b-a7eff5a9ac32,f849adc7-a8ff-55d8-84d9-596c300b878b","assetName":"1756-L75/B LOGIX5575,1756-L75/B
LOGIX5575 (Port1-Link00),Rockwell
10.17.10.52","assetIpAddress":"10.17.10.52","assetMacAddress":"00:00:bc:2d:21:27","assetVendor":"Rockwe
ll
Automation","assetProductId":"0x60","assetSerialNumber":"008a6d2a","assetDeviceType":"Controller,Engine
ering Station","assetSwRevision":"26.12","assetHwRevision":"","assetProtocol":"ARP, CIP-IO, DNS,
EthernetIP, FTP, HTTP, Netbios, SMB,
Telnet,EthernetIP","assetCustomAttributes":[],"assetConnectedLinks":[]}} [caller=endpoint.go:118]
```

To view the Cisco Cyber Vision attributes for a particular endpoint in ISE, do the following:

1. From the ISE web UI, navigate to **Content Visibility -> Endpoints**.

2. Search for an endpoint and click the link under the **MAC Address** column.



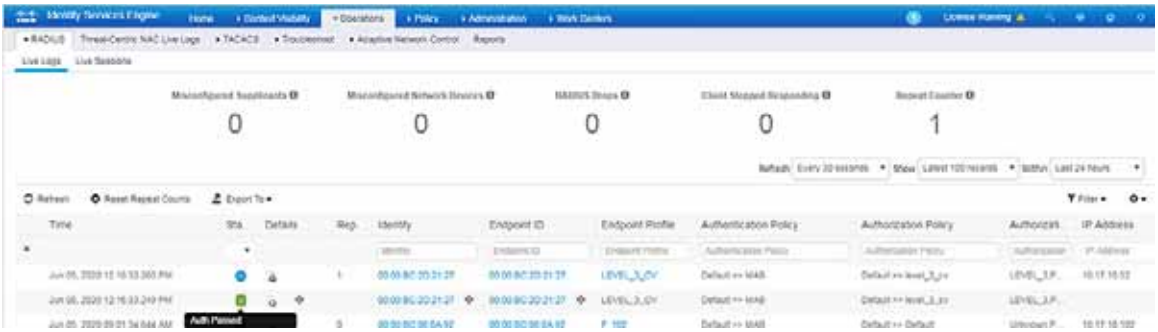
3. Verify the Cisco Cyber Vision attributes are present.

assetDeviceType	Controller,Engineering Station
assetId	1e276520-7972-5ea1-9467-08a13af01b18,d52e4e10-4da5-5998-b01b-a7eff5a9ac32,f849adc7-a8ff-55d8-84d9-596c300b878b
assetIpAddress	10.17.10.52
assetMacAddress	00:00:bc:2d:21:27
assetName	1756-L75/B LOGIX5575,1756-L75/B LOGIX5575 (Port1-Link00),Rockwell 10.17.10.52
assetProductId	0x60
assetProtocol	ARP, CIP-IO, DNS, EthernetIP, FTP, HTTP, Netbios, SMB, Telnet,EthernetIP
assetSerialNumber	008a6d2a
assetSwRevision	26.12
assetVendor	Rockwell Automation

Things to check if the profiling is incorrect or the attributes are not present:

- The profiling policy rules are accurate, including the certainty factor.
- The endpoint is successfully authenticated to ISE.

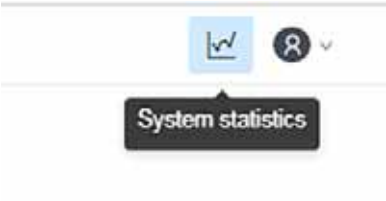
```
Switch#show access-session int gi1/3
Interface               MAC Address    Method  Domain  Status Fg  Session ID
-----------------------------------------------------------------------------------------
Gi1/3                   0000.bc2d.2127 mab     DATA    Auth        9D0F110A0000001476743B27
```



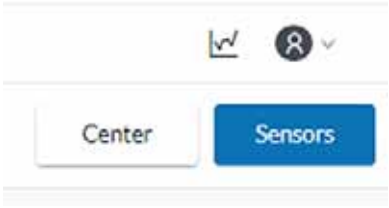
Cisco Cyber Vision Sensor Performance

To view the performance metrics of the Cisco Cyber Vision Sensors, do the following:

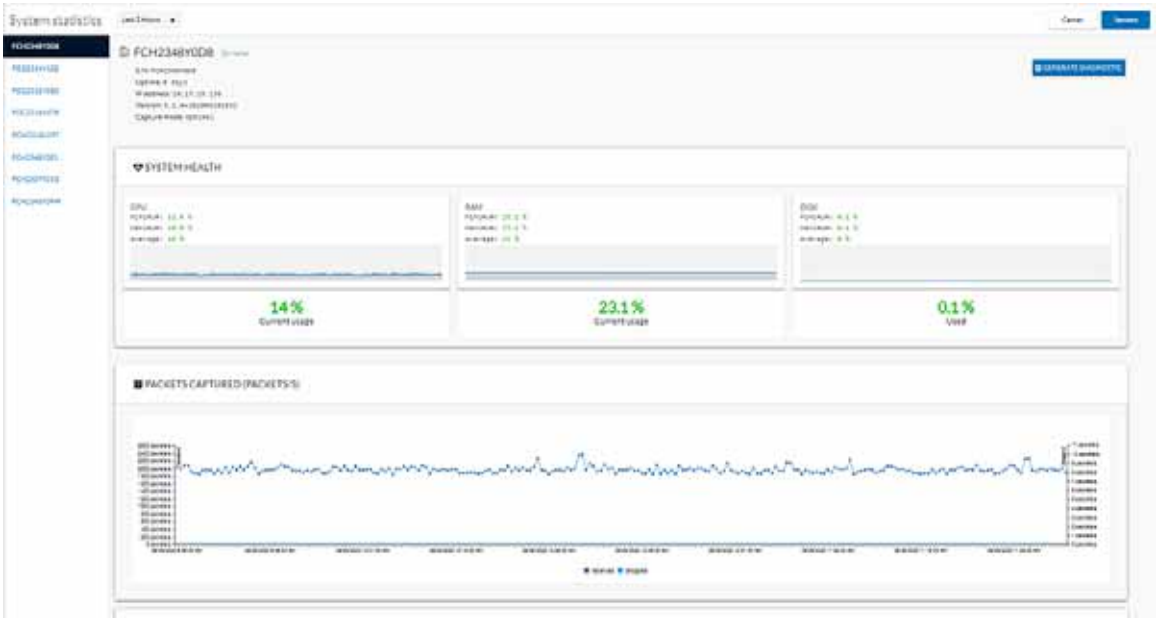
1. From the Cisco Cyber Vision Center web UI, click the **System Statistics** icon at the top right of the page.



2. Click the **Sensors** button.



3. On the left side of the page is the list of Cisco Cyber Vision Sensors. Click one of the links to view the performance details for that particular Sensor. This page provides CPU and memory usage, as well as data throughput, including any dropped packets.



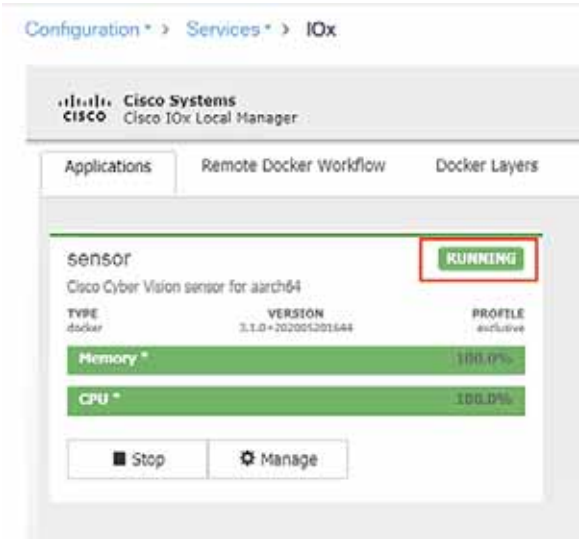
Cisco Cyber Vision Sensor Components

If components are not showing for a particular Cisco Cyber Vision Sensor, check the following:

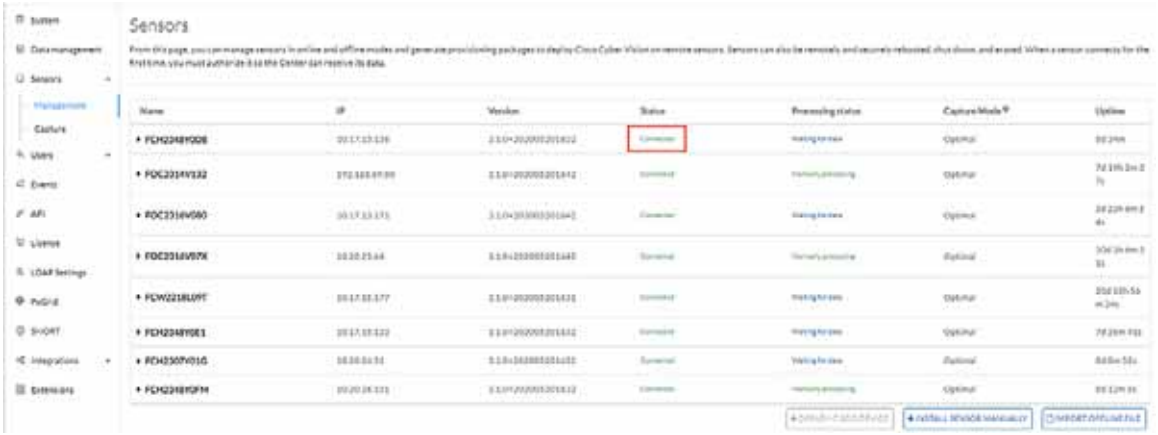
- The Cisco Cyber Vision Sensor application is running.
  - From the switch CLI:

```
Switch#show app-hosting list
App id                                   State
---------------------------------------------------------
sensor                                   RUNNING
```

– From the switch web UI under **Configuration -> Services -> IOx**:



- The switch can ping the Cisco Cyber Vision Center eth 1 interface IP address.
- In the Cisco Cyber Vision Center web UI under **Admin -> Sensors -> Management**, the **Status** column for the particular Sensor shows as “Connected”.



- The switch system time is the same as the Cisco Cyber Vision Center system time.

```
Center#date
Fri Jun  5 15:51:47 UTC 2020

Switch#show clock
11:51:47.841 EDT Fri Jun 5 2020
```

- The switch ERSPAN configuration has the correct details, including appropriate source interface(s) or VLAN(s).

```
Cat9300#show monitor session 1
Session 1
---------
Type                        : ERSPAN Source Session
Status                      : Admin Enabled
Source Ports                :
    Both                    : Gi1/0/14-15,Gi1/0/24,Gi1/1/4,Te1/1/1,Gi2/0/11,Gi2/0/24,Gi2/1/2,Te2/1/1
Destination IP Address      : 169.254.1.2
```

```
MTU                      : 9000
Destination ERSPAN ID    : 2
Origin IP Address        : 169.254.1.1
```

Site-wide Precision Time Protocol Troubleshooting

Syslog:
https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie3000/software/release/12-2_52_se/configuration/guide/ie3000scg/swlog.pdf

Table 16 PTP Debug CLI

Command	Purpose
`debug ptp {bmc | clock-correction | errors | event | messages | error | transparent-clock}`	Debug PTP events and messages: ■ bmc—Display the PTP best primary clock algorithm debug messages. ■ clock-correction—Display the PTP clock-correction messages. ■ error— Display the PTP error debug messages. ■ Event—Display the PTP state event debug messages. ■ messages—Display the PTP state event debug messages. ■ transparent-clock—Display the PTP transparent-clock debug messages.

Table 17 PTP CLI Showing Configuration and Status

Command	Purpose
`show ptp {clock | foreign-master-records | parent | port {FastEthernet | GigabitEthernet} | time-property }`	Specifies the PTP information to display: ■ clock—Displays PTP clock information. ■ foreign-master-records—Displays PTP foreign-master-records. ■ parent—Displays PTP parent properties. ■ port FastEthernet—Displays PTP properties for the FastEthernet IEEE 802.3 interfaces. ■ port GigabitEthernet—Displays PTP properties for the GigabitEthernet IEEE 802.3z interfaces. ■ time-property—Displays PTP clock-time properties.

Third-party PTP-related Equipment and Application Troubleshooting Resources

Meinberg LANTIME Configuration and Management Manual
https://www.meinbergglobal.com/download/docs/manuals/english/ltos_6-24.pdf

Previous and Related Documentation

This design and implementation guide is an evolution of a significant set of industrial solutions issued by Cisco. In many ways, this document amalgamates many of the concepts, technologies, and requirements that are shared in industrial solutions. The vertical relevance will be maintained, but shared technical aspects are essentially collected and referred to by this document.

- The existing documentation for manufacturing and oil and gas can be found on the Cisco Design Zone for Industry Solutions page:
  https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-industry-solutions/index.html
- The Cisco Catalyst 9300 and Cisco Catalyst 3850 are positioned as the distribution switches where there is a controlled IT environment.
  - Cisco Catalyst 3850 product page:
    https://www.cisco.com/c/en/us/products/switches/catalyst-3850-series-switches/index.html
  - Cisco Catalyst 9000 switching product page:
    https://www.cisco.com/c/en/us/products/switches/catalyst-9000.html
- Cisco Catalyst 3850 StackWise–480 configuration:
  - For Cisco Catalyst 3850
    https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/3se/ha_stack_manager/configuration_guide/b_hastck_3se_3850_cg/b_hastck_3se_3850_cg_chapter_010.html#reference_5415C09868764F0FA05F88897F108139
  - For Cisco Catalyst 9300
    https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/16-5/configuration_guide/stck_mgr_ha/b_165_stck_mgr_ha_9300_cg/managing_switch_stacks.html
- Industrial Ethernet switching product page:
  https://www.cisco.com/c/en/us/products/switches/industrial-ethernet-switches/index.html
- Cisco IE 3x00 Series Switch
  https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie3X00/software/16_10/release_note/b_1610_releasenote.html
- Cisco IE 4000, Cisco IE 4010, and Cisco IE 5000:
  - Switch Software
    https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie4010/software/release/15-2_4_EC/configuration/guide/scg-ie4010_5000.html
  - Switch Software Smartport configuration
    https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie4010/software/release/15-2_4_EC/configuration/guide/scg-ie4010_5000/swmacro.html
- Cisco Industrial Network Director:
  - http://www.cisco.com/go/ind
  - Network Management for Operational Technology in Connected Factory Architectures
    https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/IND/IND_Connected_Factory_CRD/IND_Connected_Factory_CRD.html
- IEC Standards:

- IEC 61588 Precision clock synchronization protocol for networked measurement and control systems http://s1.nonlinear.ir/epublish/standard/iec/onybyone/61588.pdf

Table 18 Previous Industry Documentation

Industry	Solution	Description
Manufacturing	Connected Factory—CPwE https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html	Solution to assist manufacturers seeking to integrate or upgrade their Industrial Automation and Control System (IACS) networks to standard Ethernet and IP networking technologies.
	Connected Factory—PROFINET https://www.cisco.com/c/en/us/solutions/industries/manufacturing/connected-factory/connected-factory-profinet.html	Solution for PROFINET-based industrial environments to integrate Cisco Industrial Ethernet switches into the automation network.
	Connected Factory—CC-Link IE https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/MELCO/CC-Link_Connected_Factory.html	Solution for CC-Link IE-based industrial environments to integrate Cisco Industrial Ethernet switches into the automation network.
	Connected Machine https://www.cisco.com/c/en/us/solutions/industries/manufacturing/connected-machines.html	Enable rapid and repeatable machine connectivity, providing business improvements such as overall equipment effectiveness (OEE) and machine monitoring.
	Connected Factory—Network Management for Operational Technology https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/IND/IND_Connected_Factory_CRD.html	Discusses the use of Cisco's Industrial Network Director application for monitoring industrial network assets and discovering automation devices within the context of the Connected Factory solution.
Oil & Gas	Connected Pipeline—Control Center https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/connected-pipeline-control-center.html	Secure, virtualized Control Center design for Oil & Gas pipeline operators, including secure remote access and operational support
	Connected Pipeline—Operational Telecoms https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/connected-pipeline-operational-telecoms.html	Best practice, secure, design guidance for Oil & Gas pipeline wide area networks and pipeline station networks. This includes networks between Control Centers, from Control Centers to pipeline stations, between pipeline stations, and inside pipeline stations
	Connected Refinery and Processing Facility https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/connected-refinery-processing-facility.html	Best practice, secure design guidance leveraging industrial wireless and mobility for next generation refining and processing