IE Switch Configurations

Configuring IE switches

Summary

Configuring industrial switches to communicate with Cisco IoT Operations Dashboard involves several stages. The key components or participants involved in the process are:

- Administrator: Configures and manages the IE switches throughout the process.
- IE switches: The device that is being prepared and connected to the Cisco IoT Operations Dashboard
- Cisco IoT Operations Dashboard: The cloud-based platform used to manage registered devices and confirm successful connectivity.

Workflow

These are the stages of configuring IE switches to establish connection with Cisco IoT OD.

1. Prepare the device: The administrator ensures the device is powered on, connected to the network, and accessible for configuration. For more information, see Prepare the device.
2. Configure the SD card and enable IOx: The administrator configures a compatible SD card and enables IOx on the device, preparing it to support IoT application deployment. For more information, see Configure the SD card and enable IOx on IE switches, on page 2.
3. Configure the device to connect to Cisco IoT Operations Dashboard: Using the IOS commands, the administrator configures the device to communicate with the IoT Operations Dashboard. For more information, see Configure IE switches for IoT Operations Dashboard connectivity, on page 3.
4. Verify the configuration on the device: The administrator checks the connection status on the device using IOS commands. For more information, see Verify configuration on the device terminal, on page 5.

5. Verify the device status in Cisco IoT Operations Dashboard: The administrator confirms that the device appears as “registered” in the Operations Dashboard. For more information, see Verify the device status on the Operations Dashboard, on page 6.

Result

The IE switch is securely connected to Cisco IoT Operations Dashboard, ready for remote management.

What's next

Configure remote sessions to manage OT assets.

Prepare IE devices

Use this task to prepare your IE devices before configuring them for SEA.

Get your devices ready for SEA configuration.

Procedure

Step 1 Attach the necessary networking cables.

Step 2 Power up the device.

Your IE devices are ready for SEA configuration.

Configure the SD card and enable IOx on IE switches

Prepare the SD card and enable IOx to allow deployment of containerized applications on Cisco IE switches.

IOx applications require the SD card in ext4 format. Shipped SD cards are formatted as FAT32 and must be reformatted.

Before you begin

- Ensure the SD card is inserted in the switch.
- Have console or SSH access to the switch CLI.

Follow these steps to configure the SD card and enable IOx:

Procedure

Step 1 Format the SD card to ext4 format:

```
format sdflash: ext4
```

Step 2 Configure the AppGigabitEthernet1/1 interface in trunk mode.

To configure AppGigabitEthernet1/1 in trunk mode, set the switchport mode to trunk and define a native VLAN. For the native VLAN, it's best to use a number that isn't likely to be used elsewhere, such as 4094. If the native VLAN is greater than 1004, the switch's VTP mode must be set to transparent to allow the VLAN to be created.

Example:

```
conf t
vtp mode transparent
vlan 4094
name app-man-native-vlan
interface AppGigabitEthernet1/1
switchport trunk native vlan 4094
switchport mode trunk
end
```

Step 3 Enable IOx.

```
conf t
iox
end
```

Step 4 Verify that IOx is running correctly.

IE-3400# **show iox-service**

Confirm all relevant services display as "Running".

```
IOx Infrastructure Summary:
---------------------------
IOx service (CAF)              : Running
IOx service (HA)               : Not Supported
IOx service (IOxman)           : Running
IOx service (Sec storage)      : Running
Libvirtd                       : Running
Dockerd                        : Running
```

The switch is ready to deploy IOx applications; the SD card is correctly formatted, interface is configured, and IOx is enabled.

What to do next

Deploy desired IOx applications as needed.

Configure IE switches for IoT Operations Dashboard connectivity

Enable IE devices to connect securely to the Cisco IoT Operations Dashboard (IoT OD).

To establish a secure connection between IE switches and the IoT Operations Dashboard, you must configure user credentials, enable necessary services, and set up secure transport profiles using device CLI commands.

Before you begin

- Ensure you have access to the switch's CLI with privilege level 15.
- Have an appropriate device profile with validated credentials ready on IoT OD.

Follow these steps to configure IE switches for IoT Operations Dashboard connectivity:

Procedure

Step 1 Create a privilege 15 user by applying the following configuration. The credentials should match the values configured in the Device Profile on the Cisco IoT Operations Dashboard:

Example:

```
conf t
username <DEVICE PROFILE USERNAME> privilege 15 algorithm-type scrypt secret <DEVICE PROFILE PASSWORD>
end
```

Step 2 Configure authentication settings and enable WSMA and HTTP services.

Note
The WSMA service requires "ip http server" to be enabled. For secure application deployment, also enable "ip http secure-server." Review the running-config on the device to avoid duplicate configuration.

```
conf t
  aaa new-model
  aaa authentication login default local
  aaa authorization exec default local

  ip http secure-server
  ip http server
  ip http authentication local

  wsma agent exec
    profile exec
  wsma profile listener exec
    transport http path /wsma/exec

  cgna gzip
  ntp server pool.ntp.org
  end
```

Note
The "ip http server" command initiates a web server on the device, accessible via port 443. If the device is exposed to the internet without firewall protection, restrict access to this web service to reduce security risks.

Step 3 Enable a secure TLS connection with the IoT Operations Dashboard using an IDA transport profile.

```
  conf t
  ida transport-profile wst
   callhome-url wss://device-us.ciscoiot.com/wst/cgna
   active
  end


  conf t
  ida transport-profile wst
   callhome-url wss://device-eu.ciscoiot.com/wst/cgna
   active
  end
```

Step 4 Configure the CGNA registration profile.

```
conf t
  cgna profile cg-nms-register
   transport-profile wst
   add-command show version | format flash:/managed/odm/cg-nms.odm
   add-command show inventory | format flash:/managed/odm/cg-nms.odm
   interval 3
   active
   url https://localhost/cgna/ios/registration
   gzip
  end
```

Note
After configuration, the device connects to IoT Operations Dashboard and triggers registration.

Step 5 (Optional) Enable DNS services if not already configured via DHCP. This is required for static IP setups without DNS server assignment.

Verify the configuration by using the ping command:

```
Switch# ping us.ciscoiot.com
```

The IE switch establishes a secure connection to the IoT Operations Dashboard and completes device registration.

What to do next

Verify device registration on the IoT Operations Dashboard and optionally on the device's terminal.

Verify configuration on the device terminal

This task helps you confirm that the device's transport profile is properly configured and able to establish a secure connection with the Cisco IoT Operations Dashboard.

After configuring the device, you must ensure that that device is able to communicate with the Operations Dashboard.

Before you begin

- Ensure you have access to the device terminal as an administrator or a user with sufficient privileges.
- Make sure the transport profile has already been configured on the device.

Procedure

Step 1 Run this command to verify the network connectivity:

Example:

```
Switch# show ida transport-profile-state all
```

```
! Verify that IDA status is connected for the "wst" transport profile
   ! Notice the line "IDA Status: Connected" in the show command output below for the "wst" transport
 profile.
   Switch#sh ida transport-profile-state all
```

```
Transport Profile 1:
Profile Name: wst
Activated at: Tue Mar 12 15:12:19 2024
Reconnect Interval: 30 seconds
keepalive timer Interval: 50 seconds
Source interface: [not configured]
callhome-url: wss://device-us.ciscoiot.com/wst/cgna
Local TrustPoint: CISCO_IDEVID_SUDI
Remote TrustPoint: [not configured]
Execution-url: http://localhost:80
Proxy-Addr: [not configured]
IDA Status: Connected
State: Wait for activation
Last successful response at Tue Mar 12 15:13:19 2024
Last failed response at Tue Mar 12 15:12:15 2024
Last failed reason: Gracefully disconnected
```

Step 2 Notice the line "IDA Status: Connected" in the show command output.

What to do next

If the IDA status is connected, proceed with remote session configurations.

Verify the device status on the Operations Dashboard

Confirm that a device has successfully moved from the Staged status to the Registered status in your IoT OD Organization after a registration attempt.

When a device submits a registration request to IoT OD and its configuration is validated, the device automatically moves from **Devices > Staged** to **Devices > Registered**. If no registration attempt occurs, the device remains listed as Staged.

Before you begin

- Ensure you have configured the device to communicate with IoT OD.
- Verify that the device has attempted registration, if applicable.

Procedure

Step 1 Log in to the IoT Operations Dashboard.

Step 2 From the **Sevices** pane, select **Application Manager**.

Step 3 Click **Devices > Registered** tab.

The device you added appears in the **Registered** tab, indicating successful registration.

What to do next

Configure your IE switches to enable IOx application deployment.