Configure the IE switch and initiate a connection with the IoT Operations Dashboard

Prerequisites for configuring the IE switch

- Ensure that the IE switch is added to the Cisco IoT OD Application Manager. For more information, see Create a device profile and add an IE switch to the Application Manager service.

Configuration steps

1. Prepare the device
2. Configure SD card and Enable IOx
3. Configure the IE3x00 Device to Connect to IoT OD
4. Verify the configuration on the device
5. Verify the device status in the IoT OD

Prepare the IE device

1. Attach the required networking cables.
2. Power up the device.

Configure SD card and enable IOx

IOx is a container hosting platform that runs on Cisco IOS XE, and it's used to install and execute several services that Cisco IoT Operations Dashboard can deliver such as Secure Equipment Access (SEA), Cisco Cyber Vision (CCV), and Edge Intelligence (EI). As a first step, we'll now configure and enable IOx.

To work with IOx applications, the IE3x00 must have an SD card in the **ext4** format. However, the SD card that is ordered as part of the shipment will be in FAT32 format. Therefore, you must reformat the SD card to **ext4**.

Use the following command:

```
format sdflash: ext4
```

Do the following:

1. Configure AppGigabitEthernet1/1 in trunk mode. Cisco recommends that you configure this trunk with a native VLAN that isn't likely to be used anywhere in the switch. It's also possible, but not required, to allow on this trunk only the VLANs needed for communication from the applications and the internet or other VLANs. If using a native VLAN number greater than 1004 like the example below, make sure that the switch is configured for "vtp mode transparent" to allow for the creation of this VLAN. With this configuration, applications will be deployed in any desired VLAN you wish the application traffic to follow.

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

2. Enable IOx.

   ```
   conf t
   iox
   end
   ```

3. Verify that IOx is running correctly.

   For example:

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

   The device displays an output similar to the following:

   ```
   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
   ```

Configure the IE3x00 switch to connect to IoT OD

We’re now going to execute a set of IOS commands on the device's CLI to establish a connection with the Cisco IoT Operations Dashboard. The Device Profile in the IoT Operations Dashboard is associated with devices such as IE switches, with a set of username / passwords for managing them. To manage the IOx Apps, the Cisco IoT Operations Dashboard requires a valid user configured with level 15 credentials on the switch in IOS XE.

1. Apply the following configuration to create a privilege 15 user.

   The credentials should match the values configured in the Device Profile in the Cisco IoT Operations Dashboard:

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

2. Configure the authentication-related settings and WSMA settings.

Note Usage of the WSMA service relies on http, therefore "ip http server" is required to be enabled in the configuration. To deploy applications securely, add “ip http secure-server” as well. review running-config on the device first. Some related configurations might be available out of the box.

   ```
   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, which can be accessed using port 443. If the device is exposed to the internet without enterprise firewall protection, it’s important to control access to this web service to prevent potential security risks. For more details on this issue and resolution, see Technote: Troubleshooting tips. For any assistance, please contact: Cisco TAC

3. Configure the IDA transport profile to enable a secure TLS connection using WebSocket to Cisco IoT Operations Dashboard using TLS with port TCP 443.

   For the US Cluster:

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

For the EU Cluster:

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

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 Once the configuration is done, the device connects to IoT OD and triggers the registration process.

5. (Optional) Enable DNS on the switch if it’s not already acquired through the DHCP server.

Note This is important if the switch is configured with a static IP and the static default gateway and not explicitly given a DNS server to use. In this example, we use a Cisco DNS. You can use any DNS server. To verify, execute the following commands:

Switch# **ping us.ciscoiot.com**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 35.84.105.79, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Ping will fail and that is expected, however it’s important to validate that the hostname has been resolved to an IP address. The configured DNS server can be checked with "show ip dns view". If the DHCP server doesn’t provide DNS, a DNS must be explicitly configured in the device. An example is provided below:

```
conf t
  ip name-server 208.67.222.222 208.67.220.220
  end
```

Verify the configuration on the device

Ensure that the configuration steps are complete and the template from CLI is pushed to the switch. Use the following commands to verify that the device is configured correctly to connect to IoT OD.

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

The device displays an output similar to this. Notice the line *IDA Status: Connected*.

```
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
```

Verify the device status on the IoT Operations Dashboard

Once a device connects with a registration request, the device configuration is recognized and validated by IoT OD, and the device automatically moves from **Devices > Staged** status to Registered status in your IoT OD Organization.

If IoT OD didn't receive any registration attempt, the IE3x00 device stays in the **Devices > Staged** list. Check the following on the device:

- Verify that the device has connectivity to the appropriate IoT OD cluster (US/EU) by using the telnet command.

  ```
  // Verify that opening a telnet session to the cluster is successful. The output should
   have "Open"

    Example:
    #telnet us.ciscoiot.com 443
    Trying us.ciscoiot.com (10.105.58.227, 443)... Open
  ```

- If you encounter problems, use the Event Log page on the device level to see the connectivity and Application Manager-related events. Use the troubleshooting tools on the device's Troubleshooting page for debugging.