Industrial Router Configurations

Prerequisites for configuring industrial routers

IR1101 devices

Ensure that your IR1101 device has IOx container keys programmed.

- Run this command:

```
Router# show software authenticity keys | i Name
```

- In the output, look for lines containing "Product Name: Cisco Services Containers". If the lines are present, the device has IOx container keys programmed.
- If the lines are missing:
  - Devices shipped before January 2020: Either disable signature verification or upgrade the device.
  - Devices shipped after January 1, 2020: No action is required, the device should have the container keys programmed by default.

Note SEA installation will fail with a signature verification error if the device has neither container keys programmed nor signature verification enabled.

Application Manager service

Ensure that the IR router is added to Cisco IoT OD Application Manager.

Configuring industrial routers

Workflow

There are the stages of configuring industrial routers to establish connection with Cisco IoT OD.

1. Prepare the device
2. Configure and enable IOx, on page 2
3. Configure the IR device to connect to IoT OD, on page 4
4. Verify configuration on the device, on page 5
5. Verify the device status on the Operations Dashboard, on page 6

Result

You have successfully configured the device to be able to communicate with the IoT OD.

What's next

Configure remote sessions

Prepare industrial routers

Use this procedure to prepare industrial routers for SEA configuration.

Procedure

Step 1 Attach the necessary networking cables.

Step 2 Power up the device.

Your industrial routers are ready for SEA configuration.

Configure and enable IOx

Perform this task to ensure that IOx applications have the necessary IP connectivity and network settings to operate effectively.

IOx is a container hosting platform that runs on Cisco IOS XE. 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).

Procedure

Step 1 Configure the VirtualPortGroup0 (VPG) Interface , DHCP Pool, and NAT rules on the device for IOx network.

a. Configure the VPG Interface. The virtual interface that connects IOx applications to IOS XE is called VirtualPortGroup0. The IOx applications need IP connectivity through the virtual interface, which includes receiving an IP address. An example configuration is given in the next line. You can change the IP address to suit your requirements. Enter these configuration commands on the router console, in the config mode.

```
! Example
  conf t
  interface VirtualPortGroup0
  description IOx Interface
  ip address 192.168.16.1 255.255.255.0
  ip nat inside
  ipv6 enable
  end
```

b. Configure the DHCP pool. When the IOx applications start, they will request an IP address via DHCP. Therefore, you need to configure a DHCP pool for IOx applications. An example configuration of IP pool and DNS server is given in the next line. You can customize this configuration to suit your requirements. Ensure that the default router IP address is the same as the IP address previously configured for the `VirtualPortGroup0` interface.

```
! Example
  conf t
  ip dhcp pool ioxpool
  network 192.168.16.0 255.255.255.0
  default-router 192.168.16.1
  dns-server 192.168.16.1 8.8.8.8
  end
```

c. Configure NAT. IOx Apps use private IP addresses obtained from DHCP. They need Network Address Translation (NAT) to access the internet. Add NAT Rules for the DHCP pool to enable IOx App traffic to access the internet.

In the example below, assume that the connection to the internet will be through Cellular 0/1/0. Make sure to change or adjust the interface if it is not Cellular 0/1/0. For example, it could be GigabitEthernet 0/0/0 or Cellular 0/3/0.

```
! Example of a NAT rule for using Cellular0/1/0 as an uplink:
  conf t
  interface Cellular0/1/0
  ip nat outside
  ip access-list extended NAT_ACL
  10 permit ip 192.168.16.0 0.0.0.255 any
  route-map RM_WAN_ACL2 permit 10
  match ip address NAT_ACL
  match interface Cellular0/1/0
  ip nat inside source route-map RM_WAN_ACL2 interface Cellular0/1/0 overload
  end
```

Step 2 Enable IOx.

```
conf t
iox
end
```

Step 3 Verify that IOx is running correctly by running this command in exec mode:

```
show iox-service
! Example 1: When IOx is up and running, both the “IOx service (CAF)” and “dockerd” will be running.
Router#sh iox-service
```

```
IOx Infrastructure Summary:
---------------------------
IOx service (CAF)          : Running
IOx service (HA)           : Not Supported
IOx service (IOxman)       : Running
IOx service (Sec storage)  : Running
Libvirtd 5.5.0             : Running
Dockerd v19.03.13-ce       : Running
```

IOx services are running on the device.

Configure the IR device to connect to IoT OD

To establish a connection with the Cisco IoT Operations Dashboard, you must run a set of IOS commands on the device's CLI. 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. 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:

```
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.

```
conf t
aaa new-model
aaa authentication login default local
aaa authorization exec default local
ip http server
ip http authentication local
ip http secure-server
wsma agent exec
profile exec
wsma profile listener exec
transport http path /wsma/exec
cgna gzip
end
```

3. Configure the IDA transport profile: 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 router if it's not already acquired through the DHCP server.

   This is important if the router is configured with a static IP and a static default gateway, and no DNS server is explicitly specified. In this example, we use a Cisco DNS. You can use any DNS server.

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

Verify configuration on the device

Use the following commands to verify that the device is configured correctly to connect to IoT OD.

Router# **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.
 Router#sh ida transport-profile-state all
 Transport Profile 1:
 Profile Name: wst
 Activated at: Fri Jun  7 07:26:42 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://192.168.16.1
 Proxy-Addr: [not configured]
 IDA Status: Connected
 State: Wait for activation
 Last successful response at Fri Jun  7 08:25:29 2024
 Last failed response:
 Last failed reason:
```

Verify the device status on the Operations Dashboard

Once IoT OD receives a registration request from a device and validates its configuration, the device automatically moves from the **Devices > Staged** status to **Registered** status in your IoT OD Organization.

Troubleshoot Issues

- If IoT OD receives a registration attempt but encounters some issues, (e.g., incorrect credentials), the IR device remains in the **Devices > Staged** list with **Configure Failure** status until IoT OD receives a registration attempt with the correct credentials.
- If IoT OD does not receive any registration attempt, the IR device remains in the **Devices** > **Staged** list.