



# Configure Telemetry

---

- [Application Telemetry Overview, on page 1](#)
- [Configure Syslog, SNMP Traps, NetFlow Collector Servers, and Wired Client Data Collection Using Telemetry, on page 1](#)
- [Criteria for Enabling Application Telemetry on Devices, on page 2](#)
- [Provision Application Telemetry Settings, on page 4](#)
- [Enable Application Telemetry for Wireless Controllers, on page 5](#)
- [Update Telemetry Settings to Use a New Cluster Virtual IP Address, on page 6](#)
- [Update Device Configuration Using Telemetry, on page 7](#)

## Application Telemetry Overview

Application telemetry allows you to configure global network settings on devices for monitoring and assessing their health.

## Configure Syslog, SNMP Traps, NetFlow Collector Servers, and Wired Client Data Collection Using Telemetry

With Cisco DNA Center, you can configure global network settings when devices are assigned to a specific site. Telemetry polls network devices and collects telemetry data according to the settings in the SNMP server, syslog server, NetFlow Collector, or wired client.

### Before you begin

Create a site and assign a device to the site. See [Create, Edit and Delete a Site](#).

---

**Step 1** Click the menu icon (☰) and choose **Design > Network Settings > Telemetry**.

**Step 2** In the **SNMP Traps** area, do one of the following:

- Check the **Use Cisco DNA Center as SNMP trap server** check box.
- Check the **Add an external SNMP trap server** check box and enter the IP address of the external SNMP trap server. The selected server collects SNMP traps and messages from the network devices.

**Step 3** In the **Syslogs** area, do one of the following:

- Check the **Use Cisco DNA Center as syslog server** check box.
- Check the **Add an external syslog server** check box and enter the IP address of the external syslog server.

**Step 4** In the **NetFlow** area, do one of the following:

- Click the **Use Cisco DNA Center as NetFlow collector server** radio button. The NetFlow configuration on the device interfaces is completed only when you enable application telemetry on the device. Select the NetFlow collector at the site level to configure the NetFlow destination server to the device.
- Click the **Add Cisco Telemetry Broker (CTB)** radio button and add the IP address and port number of the Cisco Telemetry Broker. The Cisco Telemetry Broker collects NetFlow records from the device and sends the information to the destination.

**Note** Cisco DNA Center must be configured as a destination in Cisco Telemetry Broker to receive NetFlow records. If Cisco DNA Center is not configured as a destination, the Application Experience does not work.

**Step 5** In the **Wired Endpoint Data Collection** area, click the **Enable Cisco DNA Center Wired Endpoint Data Collection At This Site** radio button to turn on IP Device Tracking (IPDT) on the access devices of the site.

If you don't want to enable IPDT for the site, click the **Disable** radio button (the default).

**Note** You must enable IPDT to preview the CLI configuration. When provisioning a device, you can preview the CLI configuration before deploying it on the device.

**Step 6** In the **Wireless Controller, Access Point and Wireless Clients Health** area, check the **Enable Wireless Telemetry** check box to monitor the health of the wireless controllers, APs, and wireless clients in your network.

**Step 7** Click **Save**.

## Criteria for Enabling Application Telemetry on Devices

Cisco DNA Center automatically enables application telemetry on all applicable interfaces or WLANs that are selected based on the new automatic interfaces or WLAN selection algorithm.

Application telemetry is pushed to WLANs that are provisioned through Cisco DNA Center.



- Note**
- The conventional tagging-based algorithm is supported and has precedence over the newer automatic interfaces or WLAN selection algorithm.
  - If you want to switch over from the automatic selection algorithm to the tagging-based algorithm, you must disable telemetry before provisioning the tagged SSIDs to the devices.

The following table provides the criteria for selecting interfaces and WLANs based on the conventional tagging-based algorithm (with **lan** keyword) and the new automatic selection algorithm for all the supported platforms:

Platform	Conventional Tagging-Based Algorithm	Automatic Selection Algorithm
Router	<ul style="list-style-type: none"> <li>• Interface description has the <b>lan</b> keyword.<sup>1,2</sup></li> <li>• Interface has an IP address other than the management IP address.</li> </ul>	<ul style="list-style-type: none"> <li>• Interface has an IP address other than the management IP address.</li> <li>• Interface is not any of the following:                             <ul style="list-style-type: none"> <li>• WAN                                     <p><b>Note</b> An interface is treated as a WAN-facing interface if it has a public IP address, and if there is a route rule with a public IP address that routes through the interface.</p> <p>In this context, a public IP address is not in a private range (for example, not in 192.168.x.x, 172.16.y.y, 10.z.z.z), or is an IP address that is not in the system's IP pools.</p> <p>Route rules can be dynamically learned. In this context, the <b>show ip route</b> command does not show a route to a public IP address that goes through this interface.</p> </li> </ul> </li> <li>• Loopback.</li> <li>• Management interface: GIGABITETHERNET0, GIGABITETHERNET0/0, MGMT0, FASTETHERNET0, or FASTETHERNET1.</li> </ul>
Switch	<ul style="list-style-type: none"> <li>• Interface description has the <b>lan</b> keyword.<sup>1, 2</sup></li> <li>• Switch port is configured as an access port.</li> <li>• Switch port is configured with the <b>switch-mode access</b> command.</li> </ul>	<ul style="list-style-type: none"> <li>• Interface is a physical interface.</li> <li>• Access port does not have neighbors.</li> <li>• Interface is not any of the following:                             <ul style="list-style-type: none"> <li>• Management interface: FASTETHERNET0, FASTETHERNET1, GIGABITETHERNET0/0, or MGMT0</li> <li>• LOOPBACK0, Bluetooth, App Gigabit, WPAN, Cellular, or Async</li> <li>• VSL interface.</li> </ul> </li> </ul>

Platform	Conventional Tagging-Based Algorithm	Automatic Selection Algorithm
Cisco AireOS Controller	WLAN profile name is tagged with the <b>lan</b> keyword. <sup>1,2</sup>	If the SSIDs are mixed, that is Local mode, Flex mode, and Fabric mode, Wireless Service Assurance (WSA) processing is enabled. If all the SSIDs are in Local mode, NetFlow is enabled.
Cisco Catalyst 9800 Series Wireless Controller with Optimized Application Performance Monitoring (APM) profile and IOS 16.12.1 and later.	WLAN profile name is tagged with the <b>lan</b> keyword. <sup>1,2</sup>	If the SSIDs are mixed—that is, central switching, Flex mode, and Fabric mode—the Cisco Application Visibility and Control (AVC) basic record is configured. If all the SSIDs use central switching, the Optimized APM record is configured.  For Cisco Catalyst 9800 Series Wireless Controllers with IOS 17.10 and later, Cisco DNA Center pushes the APM profile, not the AVC basic profile, for flex and fabric SSIDs.
	<b>Note</b> If you want to update the telemetry configuration, you must disable telemetry and then enable it after making the configuration changes.	
Cisco DNA Traffic Telemetry Appliance with Optimized APM profile and IOS 17.3 and later.	<ul style="list-style-type: none"> <li>Interface description has the <b>lan</b> keyword.<sup>1,2</sup></li> <li>Interface is a physical interface.</li> </ul>	<ul style="list-style-type: none"> <li>Interface is a physical interface.</li> <li>Interface is not a management interface: GIGABITETHERNET0, GIGABITETHERNET0/0, MGMT0, FASTETHERNET0, and FASTETHERNET1.</li> </ul>

<sup>1</sup> The **lan** keyword is case insensitive and can be separated by a space, hyphen, or underscore.

<sup>2</sup> Resynchronize the network device to read the **lan** interface description.

## Provision Application Telemetry Settings

Configure global telemetry settings as described in [Configure Syslog, SNMP Traps, NetFlow Collector Servers, and Wired Client Data Collection Using Telemetry, on page 1](#).

**Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.

The Inventory window displays the device information gathered during the discovery process. To view devices available in a particular site, expand the Global site in the left pane and select the site, building, or floor.

**Step 2** Choose the devices that you want to provision.

**Step 3** From the **Actions** drop-down list, choose **Telemetry** and do one of the following:

**Note** The application telemetry option is enabled only if the device supports application telemetry enablement from Cisco DNA Center.

- Enable Application Telemetry:** To configure application telemetry for the selected devices.
- Disable Application Telemetry:** To remove the application telemetry configuration from the chosen devices.

**Step 4** Click **Apply**.

The **Application Telemetry** column shows the telemetry configuration status. If you don't see the **Application Telemetry** column in the default column setting, click the ellipsis icon (⋮) at the right end of the column headings and check the **Application Telemetry** check box.

---

## Enable Application Telemetry for Wireless Controllers

You can enable application telemetry for new and existing devices.

### Before you begin

To enable application telemetry, devices must have a Cisco DNA Advantage license.



---

**Note** Before enabling application telemetry in Cisco DNA Center, ensure to delete any existing flow monitors configured manually from **Configuration > Services > Application Visibility > Flow Monitors** through the Cisco Catalyst 9800 Series Wireless Controller GUI.

---

- 
- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
- Step 2** To view devices available in a particular site, expand the **Global** site in the left pane, and choose the site, building, or floor.
- Step 3** In the **Inventory** window, choose the device. You can choose multiple devices at a time.
- Step 4** From the **Action** drop-down list choose **Telemetry > Enable Application Telemetry**.
- Step 5** In the **Enable Telemetry** slide-in pane, complete the following settings:
- AP mode: Check the **Flex/Fabric** or **Local** check box. You can also choose both options.
  - Check the **Include Guest SSID** check box to enable telemetry for guest SSIDs.
  - Telemetry Source:**
    - Embedded Wireless Controllers - NetFlow
    - AireOS wireless controller (Local mode) - NetFlow
    - AireOS wireless controller (Flex/Fabric mode) - Wireless Service Assurance (WSA)
  - To apply the same settings for all wireless controllers, check **Apply this selection to all wireless controllers**.
- Step 6** Click **Enable**.
- Step 7** In the **Application Telemetry** window, click **ok**.
- To skip this screen in the future, check **Don't show again**.
- The telemetry status is shown in the **Application Telemetry** column in the **Inventory** window.
-

# Update Telemetry Settings to Use a New Cluster Virtual IP Address

If you are using the Cisco DNA Center application telemetry to monitor device data, and you need to change the Cisco DNA Center cluster virtual IP address (VIP), complete the following steps to change the VIP and to ensure that node telemetry data is sent to the new VIP.

## Before you begin

- Determine the version of Cisco DNA Center that you are using. You can check this by logging in to the Cisco DNA Center GUI and using the **About** option to view the Cisco DNA Center version number.
- Obtain SSH client software.
- Identify the VIP address that was configured for the 10-GB interface facing the enterprise network on the Cisco DNA Center primary node. Log in to the appliance using this address, on port 2222. To identify this port, see the rear-panel figure in the "Front and Rear Panels" section in the [Cisco DNA Center Installation Guide](#).
- Obtain the Linux username (**maglev**) and password configured on the primary node.
- Identify the cluster VIP that you want to assign. The cluster VIP must conform to the requirements explained in the "Required IP Addresses and Subnets" section in the [Cisco DNA Center Installation Guide](#).

---

**Step 1** Access the Cisco DNA Center GUI and disable Application Telemetry at all the sites, as follows:

- a) Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.

The Inventory window displays the device information gathered during the discovery process. To view devices available in a particular site, expand the Global site in the left pane, and select the site, building, or floor.

- b) Choose all the sites and devices currently being monitored.  
c) From the **Actions** drop-down list, choose **Telemetry > Disable Application Telemetry**.  
d) Wait for the sites and devices to show that telemetry has been disabled.

**Step 2** Use the appliance Configuration wizard to change the cluster VIP, as follows:

- a) Using an SSH client, log in to the VIP address that was configured for the 10-GB interface facing the enterprise network on the Cisco DNA Center primary node. Be sure to log in on port 2222.  
b) When prompted, enter the Linux username and password.  
c) Enter the following command to access the Configuration wizard on the primary node:

```
$ sudo maglev-config update
```

If you are prompted for the Linux password, enter it again.

- d) Click **[Next]** until the screen prompting you for the cluster virtual IP appears. Enter the new cluster VIP, then click **[Next]** to proceed through the remaining screens of the wizard.

You must configure one virtual IP per configured interface. We recommend that you enter the `sudo maglev-config update` command so that the wizard prompts you to provide one VIP per configured interface.

When you reach the final screen, a message appears, stating that the wizard is ready to apply your changes.

- e) Click [**proceed**] to apply the cluster VIP change.

At the end of the configuration process, a success message appears and the SSH prompt reappears.

**Step 3** Restart the necessary Cisco DNA Center services by entering the following series of commands at the SSH prompt:

```
magctl service restart -d collector-netflow
magctl service restart -d collector-syslog
magctl service restart -d collector-trap
magctl service restart -d wirelesscollector
```


**Step 4** Wait for all the services to restart. You can monitor the progress of the restarts by entering the following command, substituting service names as needed for the release train appropriate for your Cisco DNA Center version.

```
magctl appstack status | grep -i -e collector-netflow -e collector-syslog -e collector-trap -e
wirelesscollector
```

When all the necessary services are running, you see command output similar to the following, with a Running status for each service that has restarted successfully:

```
assurance-backend wirelesscollector-123-bc99s 1/1 Running 0 25d <IP> <IP>
ndp collector-netflow-456-lxv1x 1/1 Running 0 1d <IP> <IP>
ndp collector-syslog-789-r0rr1 1/1 Running 0 25d <IP> <IP>
ndp collector-trap-101112-3pp1lm 1/1 Running 0 25d <IP> <IP>
```


**Step 5** Access the Cisco DNA Center GUI and **Enable Application Telemetry** to all nodes as follows:

- Click the menu icon () and choose **Provision > Network Devices > Inventory**.
- Choose all the sites and devices that you want to monitor.
- From the **Actions** drop-down list, choose **Telemetry > Enable Application Telemetry**.
- Wait for the sites and devices to show that telemetry has been enabled.

---

## Update Device Configuration Using Telemetry

You can push configuration changes to a device regardless of whether device controllability is enabled or disabled.

**Step 1** Click the menu icon () and choose **Provision > Network Devices > Inventory**.

The Inventory window displays the device information gathered during the discovery process. To view devices available in a particular site, expand the **Global** site in the left pane, and select the site, building, or floor.

**Step 2** Choose the devices on which you want to update the configuration changes.

**Step 3** From the **Actions** drop-down list, choose **Telemetry > Update Telemetry Settings**.

The **Update Telemetry Settings** slide-in pane appears.

**Step 4** (Optional) Check the **Force Configuration Push** check box to push the configuration changes to the device.

If there is no change in the configuration settings, the existing configuration is pushed again to the device.

**Step 5** Click **Next**.

**Step 6** Based on the Visibility of Configurations settings, choose an available option. For more information, see [Visibility of Configurations Workflow](#).

- To immediately deploy the configuration, click the **Now** radio button.
- To schedule the task for a later date and time, click the **Later** radio button and define the date and time of the deployment.
- Cisco DNA Center allows you to review the configurations before deploying them on Cisco network devices. The configuration can be reviewed from the **Preview Configuration** window.

To preview the CLI configuration, click the **Generate configuration preview** radio button.

**Note** During configuration preview, the PKCS12 certificate isn't generated as the certificate must be used within 15 minutes. The **Preview Configuration** window only displays the relevant configuration commands. When you deploy the configuration after previewing it, the PKCS12 certificate is generated and pushed to the device.

**Step 7** Click **Apply**.

---