Telemetry

Cisco IoT FND enables seamless telemetry integration with CDNA and supports both online and offline data transfer modes. Cisco IoT FND collects telemetry data and ensures reliable delivery to CDNA, regardless of network connectivity conditions. Here are some ways in which you can use telemetry:

- in online mode, Cisco IoT FND collects and immediately pushes telemetry data to CDNA in real time.
- in offline mode, Cisco IoT FND stores telemetry data locally and uses an Amazon Web Server (AWS)-based offline connector to upload the data to CDNA when connectivity is available.
- telemetry ensures continuous and dependable telemetry data transfer across diverse network environments.

Table 1: Feature history

Feature name	Release information	Description
Telemetry	Cisco IoT FND 5.1	Cisco IoT FND supports flexible telemetry data integration with Cisco DNA Center (CDNA), enabling seamless data transfer in both online and offline modes.

Benefits

- Telemetry helps you automatically track and report on regulatory compliance by continuously monitoring configuration changes and network activity.
- By analyzing telemetry data, you can identify underutilized or overburdened network resources, enabling smarter allocation and cost savings.
- Telemetry allows you to observe long-term patterns and trends in network behavior, supporting better forecasting and strategic planning.

Prerequisites

Here are some of the prerequisites to use telemetry:

- Ensure that the server running Cisco IoT FND is connected to the internet when operating in online mode.
- You need to be a root user to access telemetry data. For more information on user access on Cisco IoT FND see, Manage user access.

Telemetry is applicable only on Cisco IoT FND running Cisco IoT FND Release 5.1 and later releases.

Restrictions

Here are some restrictions of telemety that you need to consider before using the feature:

- Only if you are a root user, you can enable or disable telemetry, add or modify proxy details and telemetry job run time for internet access in case Cisco IoT FND is unable to reach Cisco telemetry.
- Cisco IoT FND runs a job daily to collect the telemetry and store it in the Cisco IoT FND database. This job is scheduled to run at 2:00AM by default. You can change the default time once you've given consent to send telemetry data.
- After you consent to sending telemetry data to CDNA and if telemetry fails for 7 consecutive days, Cisco IoT FND stops collecting and pushing telemetry data. You as a root user has to enable telemetry using Cisco IoT FND once again.
- Telemetry data is retained in Cisco IoT FND only for 7 days before being auto-deleted.

Configure telemetry

This task guides you in providing consent to extract Cisco IoT FND telemetry data for reporting and improving your experience.

Before you begin

Log in as a root user

Use these steps to configure telemetry on your Cisco IoT FND:

Procedure

Step 1 Log in to Cisco IoT FND as a root user.

Step 2 In the **Telemetry Acceptance** page, confirm that you are accepting to extract Cisco IoT FND telemetry data. Check the **Accept** check box.

Field	Field description
Customer Name	Enter your organization's name.

Field	Field description
Proxy URL	Enter the Proxy settings URL to reach cisco telemetry
Proxy Username	Enter Proxy user name
Proxy Password	Enter Proxy password

Step 3 Click the **save** icon.

Step 4 If you don't want to consent to extracting telemetry data, click **Reject**.

Step 5 The **Telemetry Acceptance** page appears only during your first login as a root user. If you'd want to accept telemetry at a later point of time, go to **ADMIN** > **Telemetry**.

You've succesfully configured telemetry on Cisco IoT FND.

Monitor telemetry

Once you've configured telemetry on Cisco IoT FND, you can view the telemetry data using this task.

Before you begin

Ensure that you've provided consent to telemetry extraction from your Cisco IoT FND

Here are the instructions to view the telemetry data

Procedure

Step 1 From the Cisco IoT FND menubar, choose **ADMIN** > **System Management** > **Telemetry**.

Step 2 You can view the following telemetry data on Cisco IoT FND:

Telemetry data	Supported Cisco IoT FND Release
Customer name	Cisco IoT FND Release 5.1
Device types registered in FND	Cisco IoT FND Release 5.1
Count of devices for each device types registered in FND	Cisco IoT FND Release 5.1
Firmware versions running on the device for each device type	Cisco IoT FND Release 5.1
Count of devices for each running firmware version for each device type	Cisco IoT FND Release 5.1
Customer type ex: AMI or DA	Cisco IoT FND Release 5.1
Customer deployment method ex: PKI or PSK	Cisco IoT FND Release 5.1
Customer installation type ex: Postgres OVA/Oracle Baremetal/Oracle OVA	Cisco IoT FND Release 5.1

Telemetry data	Supported Cisco IoT FND Release
Database version	Cisco IoT FND Release 5.1
Number of config groups(count) and firmware groups(count)	Cisco IoT FND Release 5.1
Number of templates for each device types	Cisco IoT FND Release 5.1
Number of open issues	Cisco IoT FND Release 5.1
Number of dashlets used by customers	Cisco IoT FND Release 5.1
Count of devices having iox enabled	Cisco IoT FND Release 5.1
Count of devices having pluggable and expansion module	Cisco IoT FND Release 5.1
Count of event and issue types	Cisco IoT FND Release 5.1
RAM allocated to FND	Cisco IoT FND Release 5.1
CPU allocated to FND	Cisco IoT FND Release 5.1
CPU allocated to FND	Cisco IoT FND Release 5.1
IPAM is enabled	Cisco IoT FND Release 5.1
Count of active, inactive and total users	Cisco IoT FND Release 5.1
Authentication type	Cisco IoT FND Release 5.1
Count of app servers	Cisco IoT FND Release 5.1
Count of domains	Cisco IoT FND Release 5.1

You've successfully verified the telemetry data.