IoT FND User Interface

This chapter provides an overview of the IoT FND user interface. From the user interface, you can manage, monitor, and troubleshoot devices, events, and issues in your FAN, and perform a variety of other administrative and management tasks.

To access the IoT FND user interface, enter the following URL in your web browser and log in with your IoT FND username and password. Replace *fnd-ip* with the IP address of your IoT FND system.

https://*fnd-ip*/login.seam

The FND user interface includes the following menus. Use these menus to access the pages in the IoT FND user interface.

- Dashboard
- Devices
- Operations
- Config
- Admin
- Apps

For more detailed information about the IoT FND user interface and the activities you can perform, see Cisco IoT Field Network Director User Guide.

- Dashboard, on page 1
- Devices Menu, on page 2
- Operations Menu, on page 3
- Config Menu, on page 3
- Admin Menu, on page 4
- Apps Menu, on page 5

Dashboard

The **Dashboard** appears when you log in to IoT FND. You also can click **DASHBOARD** to display the Dashboard.

This page displays dashlets that provide information about the FAN, including the operational states and operational trends of routers, endpoints, and gateways. Actions that you can perform on this page include:

- Use the configurable and customizable dashlets to view information in various formats, such as pie charts, bar charts, or line graphs.
- Add, minimize, refresh, export, reposition, and remove dashlets as needed.
- Use the **Filter** option to view information for a specific time or time period.
- Export selected information in Excel format for archiving and analysis.
- Use the **Series Selector** option to display information by device status.

Devices Menu

The **Devices** menu provides access to pages that list and provide information about the devices and assets that you can manage with IoT FND. The pages also provide options for performing most onboarding and lifecycle management activities, including adding items, deleting items, and changing item properties.

To display the Devices menu, click **DEVICES**. This menu includes the following options:

- **Field Devices**: Displays information about the field area routers, endpoints, and gateways that are managed in IoT FND and provides options for managing devices.

  You can add devices for IoT FND to manage, remove devices from IoT FND management, manage labels that identify a set of devices, modify device properties, refresh the display of device metrics, block devices from accessing IoT FND, remove devices from IoT FND management, troubleshoot devices, and perform other related tasks. You also can monitor devices in real-time, obtain information about the health of devices, and view detailed hardware, software, and metrics information for a device. The Map view displays the geographical location of each device.

- **Head End Routers**: Displays information about the HERs that are managed with IoT FND and provides options for managing these devices.

  You can add HERs for IoT FND to manage, remove HERs from IoT FND management, manage labels for devices, trace routes to a device, and perform other related tasks. You also can view detailed hardware, software, and metrics information for a HER, and view information about tunnels that are established between HERs and FARs.

- **Servers**: Displays information about the IoT FND application and database servers and provides options for managing these servers.

  You can ping servers, remove servers, and add or remove labels for servers. You also can view detailed hardware, software, and metrics information for a server.

- **Assets**: Displays information about third-party equipment that is associated with IoT FND managed devices and provides options for managing this equipment. Assets can include routers, meters, extenders, access points, cameras, and other similar devices.

  You can add assets to be managed by IoT FND, remove assets from IoT FND management, change the properties of assets, and add files such as images to assets.

Operations Menu

The **Operations** menu provides access to pages with options for monitoring events, issues, and tunnel status in your network.

To display the **Operations** menu, click **OPERATIONS**. This menu includes the following options:

- **Events**: Displays notifications about events that are associated with IoT FND-managed devices. Events include activities, warnings, state changes, or errors that IoT FND detects on devices. An event can be the result of a user action, for example, provisioning a tunnel. It also can be the result of a problem with a device, for example, a low battery, expired certificate, or metric retrieval failure. An event notification includes the time period in which the event occurred, and other related information that can help you address an issue.
- **Issues**: Displays information about the overall health of the network, and displays a list of issues, which are unresolved events. Major and critical issues appear at the top of the screen, and you can view issues for the periods of your choice.
- **Tunnel Status**: Provides information about tunnels that have been provisioned between HERs and FARs.

Config Menu

The **Config** menu provides access to pages with options for configuring devices, installing firmware on devices, managing device files, provisioning tunnels, managing rules, and managing groups.

To display the **Config** menu, click **CONFIG**. This menu includes the following options:

- **Device Configuration**: IoT FND lets you configure devices by using configuration templates and configuration groups. A configuration template contains configuration settings for devices, and a configuration group is a collection of similar devices. By pushing a configuration template to a configuration group, you can apply the same settings to all devices that are in that configuration group. This approach is an efficient way to configure many devices with a single operation.

  You can view and access configuration templates and configuration groups, add devices to configuration groups, edit configuration templates, push configuration templates to devices, and manage configuration group properties.
- **Firmware Update**: Provides options for installing a firmware image on a router or endpoint. This page also displays information about the firmware that is installed on devices, firmware images that are available for devices, and information about subnets for endpoints.

  You can install a firmware image on a single device or use predefined or user defined firmware groups to install a firmware image on several devices with a single operation. You can also upload WPAN images to IoT FND.
- **Device File Management**: Provides options for viewing and managing device files. These files include configuration files, log files, and debug files on devices.
- **Rules**: Provides options for adding, activating, deactivating, and deleting rules, and displays information about existing rules. A rule defines actions that IoT FND performs after specified events occur or when it receives metrics that match criteria that you define. Use a rule to specify a message and severity to include in the log entry for an event.

- **Tunnel Provisioning**: Provides options for provisioning tunnels between HERs and FARs. You also can configure the bootstrap configuration templates for HERs and FARs and view the bootstrap status of a router during plug and play (PNP) operation.
- **Groups**: Provides options for managing endpoint groups, which are a logical groupings of devices. You can add endpoints to groups, remove endpoints from groups, and move an endpoint to another group.

  Groups provide a convenient way to manage several endpoints at one time. For example, when you push a configuration to a group, IoT FND pushes the configuration to all the endpoints in that group.

Admin Menu

The **Admin** menu provides access to the **Access Management** pages and the **System Management** pages.

The **Access Management** pages provide options for configuring various user access and device domain settings and display related information. The **System Management** pages provide options for configuring various user login, security, logging, provisioning, and server options, and display related information.

To display the **Admin** menu, click **ADMIN**. This menu includes the following options:

Access Management Pages

- **Users**: Provides options for managing IoT FND user accounts, including adding users, deleting users, activating users, deactivating users, and updating user roles.
- **Roles**: Provides options for managing roles that you can assign to IoT FND users.

  Each user is assigned a role, and the role determines what IoT FND operations the user can perform based on permissions that are enabled for a role. You can view existing roles, modify the permissions that are enabled for default roles, create new roles and enable permissions for them as needed, and delete non-default roles.
- **Domains**: Provides options for managing domains.

  A domain is a logical grouping of devices within the network, and it is used in multi-tenancy environments where a single deployment of IoT FND can support multiple customers. You also add and delete domains, update domain configuration, configure the hierarchy for a domain, and designate the IoT FND users who can modify information in a domain.
- **Password Policy**: Provides options for configuring the conditions that valid IoT FND user passwords must meet. This page also provides an option for setting the number of consecutive unsuccessful log in after which the user is locked out from IoT FND. An administrator must grant a locked out user permission to log in again.
- **Authentication**: Provides options for configuring the type of authentication that IoT FND uses to verify a user before the user can log in, and for configuring parameters for user authentication methods. You can configure local authentication, local or remote authentication, or single sign-on (SSO) authentication.

  With local authentication, user credentials stored in the IoT FND database. With remote authentication, user credentials are stored in a RADIUS server. With SSO authentication, user credentials are stored in an identify provider (IdP).

System Management Pages

- **Active Sessions**: This screen displays information about each user who is logged in to IoT FND, including the IP address of the user device, the date and time that the user logged in, and the date and time that the user last accessed IoT FND. The root user can force logout other users from IoT FND.
- **Audit Trail**: Provides information about the IoT FND activities that each user performed, including when the user logged in and what operations the user performed.
- **Certificates**: Provides options for viewing and downloading CoAP Simple Management Protocol (CSMP), router certificates, or web certificates. Devices use these certificates to ensure secure communication in the network. You also can add a trust anchor to the default profile for a Cisco IOx device that is managed by IoT FND.
- **Data Retention**: Provides options for designating the number of days that IoT FND stores information about events, issues, and metrics. Data is permanently deleted after the designated retention period.
- **License Center**: Provides options for viewing and managing IoT FND license files.
- **Logging**: Provides options for downloading IoT FND log files and for configuring the log level for logging categories. Log files capture information about events that occur on devices that are managed by IoT FND.
- **Syslog Settings**: Provides options for enabling IoT FND to send information about events to a syslog server, and for designating the syslog server to which events are sent.
- **Provisioning Settings**: Provides options for configuring the DHCPv4 and DHCPv6 proxy client settings that IoT FND requires to create tunnels between FARs and HERs and for configuring the URL of the IoT FND server.
- **Server Settings**: Provides options for viewing and managing IoT FND server settings. Items that you can configure include keystore settings for downloading log files, the timeout period after which IoT FND terminates web sessions, the period after which IoT FND moves unreachable devices to the Down state, the start day of monthly billing periods for cellular and ethernet (satellite) services, RPL tree settings, and map settings.
- **Jobs**: Displays the state and execution status of IoT FND jobs. A job is an IoT FND operation that you performed. Examples of jobs include provisioning a tunnel, updating firmware, or pushing a configuration file to devices.

Apps Menu

The **Apps** menu provides access to pages with options for managing Docker applications that are installed on Cisco 1800 Series Industrial Integrated Services Routers and Cisco Catalyst IR1100 Rugged Series Routers. Activities that you can perform include installing, uninstalling, starting, stopping, and exporting applications.

Note This menu is available only for the IoT FND VM deployment with Postgres.