



SmartHub INFER™



User Guide

Last updated on June 20, 2025

Find out more about our products and solutions at <https://www.smarthub.ai>

Copyright ©2025 SmartHub Inc. All rights reserved.

Table of Contents

1	Introduction	6
1.1	Navigating the INFER™ Console	6
1.2	Document Conventions	7
1.3	System Requirements	7
1.4	Browser Support	8
1.5	Privacy Notice	8
1.6	Trademarks	8
2	Configuring Your Organization	9
2.1	Roles and Permissions	9
2.2	Users	12
2.3	Groups	13
2.4	Roles	15
3	Space Management	17
3.1	Smart Spaces	17
3.2	Use Cases	17
3.3	Create a Space Template	18
3.4	Editing a Space Template	20
3.5	Assigning a Parent Template	20
3.6	Cloning a Space Template	21
3.7	Deleting a Space Template	22
4	Working with an Asset as a Template	24
4.1	What is an Asset?	24
4.2	What is an Asset Template?	24
4.3	What are Asset Properties?	25
4.4	What are Metrics?	25
4.5	INFER™ Agent Daemon	25
4.6	What is an Adapter?	26
4.7	Connected Asset Templates	26
4.8	Creating an Asset Template	27
4.9	Editing an Asset Template	30
4.10	Adding a Child Template	31
5	Onboarding Gateways	33
5.1	What is a Gateway?	33
5.2	Onboarding a Gateway using Basic Authentication	35
5.3	Onboarding a Gateway using Token-Based Authentication	36
5.4	Onboarding a Gateway using Property-based Authentication	37
5.5	Onboarding a Gateway using TPM-based Authentication	38
5.6	Onboarding a Gateway using Zero Touch Enrollment	40
5.7	Re-enrollment of a Gateway	41
5.8	Whitelisting an Asset	42
5.9	Using Package Management CLI to Register Multiple Assets	42
5.10	Registering Multiple Gateways	44
6	Working with INFER™ Agent	47
6.1	Installing INFER™ Agent	47
6.2	Working with IoTCAgent CLI	54
6.3	Updating INFER™ Agent	55
6.4	Uninstalling INFER™ Agent	57
6.5	Firmware Updates for an Asset	58
7	Onboarding Connected Things	59
7.1	Registering Things One by One	59

7.2	Registering Things in Bulk	62
8	Spaces	65
8.1	Creating Spaces	65
8.2	Editing Spaces	66
8.3	Assigning Spaces to assets	66
8.4	Unassigning Spaces to Assets	69
8.5	Assigning / Unassigning Parent Spaces	70
8.6	Bulk Assign Spaces to Assets	72
8.7	Deleting Spaces	74
9	Working with Insights	76
9.1	Viewing Dashboards	76
9.2	Customizing Dashboards	78
9.3	Downloading Data from Table Panels	79
10	Working with All Assets	81
10.1	Adding Assets	82
10.2	Understanding Asset Information	86
10.3	Bulk Edit Custom Properties	89
10.4	Assign Space	90
10.5	Connect to Parent	90
11	Working with Assets	92
11.1	Sending Commands to INFER™ Agent	92
11.2	Sending Commands to Multiple Assets	92
11.3	Bulk Command Cancellations	94
11.4	Asset States	94
11.5	Asset Maintenance	94
11.6	Asset Migration	96
11.7	Unenrolling Assets	98
11.8	Deleting Single or Multiple Assets	99
11.9	Viewing List of Files	99
11.10	Viewing List of Assets by Property	99
11.11	Updating Bulk Custom Properties on Multiple Assets	100
11.12	Editing Custom Properties via Spreadsheet	101
11.13	Collecting Metrics using DefaultClient Binary	103
11.14	Viewing Metric Graphs	103
12	Working with Campaigns	105
12.1	What is a Campaign?	105
12.2	Campaign Approvals	107
12.3	Campaign State Transition Scheme	108
12.4	Creating a Campaign	108
12.5	Starting a Campaign	110
12.6	Cloning a Campaign	111
12.7	Editing a Campaign	112
12.8	Deleting a Campaign	112
12.9	Controlling Campaigns using DefaultClient CLI	113
13	Working with Package Builder	117
13.1	What is a Package?	117
13.2	Creating a Package using Package Builder	117
14	Package Management CLI for Advanced Users	121
14.1	Creating a Specification YML File	121
14.2	Lifecycle Phases	124
14.3	Downloading the Package Management CLI Tool	125
14.4	Generating an IoTCP Package	125

14.5	Sample Script for Running a Campaign on a Thing Device	128
15	Working with Alerts & Notifications	130
15.1	What is an Alert?	130
15.2	What is an Alert Definition?	131
15.3	Creating an Alert Definition	132
15.4	Editing Alert Definitions	135
15.5	Disabling Alert Definitions	136
15.6	Enabling Alert Definitions	136
15.7	What is a Notification?	137
15.8	What is a Notification Definition?	138
15.9	Creating a Notification Definition	138
15.10	Editing Notification Definitions	140
15.11	Cloning Notification Definitions	141
15.12	Deleting Notification Definitions	141
15.13	Sending Notifications to ServiceNow	142
15.14	Sending Notifications to Microsoft Teams	143
15.15	Sending Notifications to Slack	144
15.16	Sending Notifications to Smartsheet	146
16	Security	148
16.1	Working with Certificates	148
16.2	Importing CA Certificate	149
16.3	Creating a Certificate Signing Request (CSR)	149
16.4	Generate CSR in Bulk	150
16.5	Signing CSR and Import Certificate	150
16.6	Importing Bulk Certificates	151
17	Working with API Keys	155
17.1	Key States	155
17.2	Creating a Key	155
17.3	Editing a Key	156
17.4	Renewing an Key	157
17.5	Revoking a Key	157
17.6	Deleting a Key	158
17.7	Viewing Key Details	159
17.8	Viewing Key Permissions	159
17.9	Viewing Key History	160
18	Settings	161
18.1	Setting up Custom Branding	161
18.2	Setting up the Default Gateway & Thing Template	161
18.3	Setting up Audit Log Retention Period	162
18.4	Setting up Identity & Access	163
18.5	Setting up Insights Dashboard	166
18.6	Setting up Notification Retention Period	167
18.7	Setting up Notification Definitions	168
18.8	System Notifications Settings	168
18.9	UI Applications	169
18.10	Setting up OTA Updates	170
19	Troubleshooting	171
19.1	Troubleshooting Campaign Management	171
19.2	INFER™ Agent Connectivity to the INFER™ Server	171
19.3	Frequently asked Questions	172
20	Integrating with Third-Party CMS	173
21	TPM-Based Attestation	174

21.1	What is Boot Attestation?	174
21.2	What is Runtime Attestation?	174
21.3	What Is Integrity Measurement Architecture?	175
21.4	Preparing Your Gateway for Boot Attestation	175
21.5	Preparing Your Gateway for Runtime Attestation	176
22	Tasks	182
22.1	Integrating with ServiceNow	182
23	SmartHub INFER™ In-Product Help	184
23.1	How to Submit a query or Report a Bug in SmartHub INFER™?	184
23.2	Landing Page within INFER™ UI	184
24	Audit Logs	186
25	Glossary	187

1 Introduction

SmartHub, Inc. is a SaaS company that offers you a complete suite of IoT Management solutions across industry verticals which ensure continuous uptime of your Edge environment.

SmartHub INFER™ is its IoT & Edge management platform designed to improve your enterprise's operational excellence and cost efficiency.

The INFER™ platform on-boards, configures, manages, monitors, and secures unmanned IoT devices and objects at scale. INFER™ enables you to pre-register and bulk onboard IoT devices, manage alerts and notifications, troubleshoot, change the configuration of devices, view audit logs, and perform compliance management operations through over the air updates.

The functionality of INFER™ can be broadly classified into the following three areas:

1. Monitoring and Alerting:

- Metric Monitoring
- Diagnostics
- Logging and Troubleshooting
- Creating Alerts on Static Thresholds
- Alert Aggregation and Clearance

2. Over The Air (OTA) Campaign:

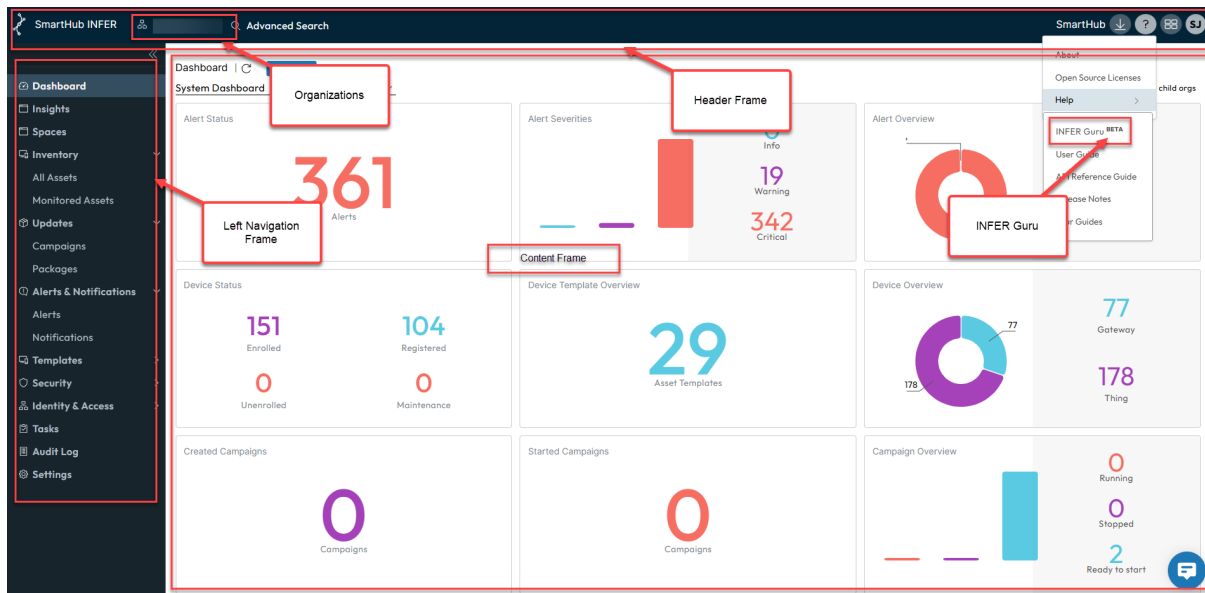
- Software, Firmware
- Operating System
- BIOS Updates
- Package Repository and
- Updates

3. Device Management and Configuration:

- Device Provisioning
- Device Enrollment
- Remote Command Execution
- File Upload to Server from Device
- Gateway Configuration

1.1 Navigating the INFER™ Console

This section describes the INFER™ Console's user interface.



The INFER™ Console uses three separate frames to display different sections of content within a single webpage.

Header Frame: This frame is placed at the top of the Console and contains the header of the INFER™ application. It includes the logo, **Organization** menu, **Advanced Search**, and other elements that are consistent across all pages.

Navigation Frame: Placed on the left side of the page, it is also called **Left Navigation Bar** in this guide. It lists INFER™'s core module as links and menus pointing you to appropriate pages of the Console. This frame remains static while the content frame changes based on your interaction.

Content Frame: This is the main section of the INFER™ Console where the primary module pages appear. This frame changes dynamically as you click different links in the left navigation bar, loading new content without refreshing the entire page.

1.2 Document Conventions

In this documentation, a greater-than symbol (>) is used to separate actions within a step and items within a cross-reference path.

A trademark symbol (®, TM, etc.) denotes a SmartHub trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as UNIX*, should use forward slashes as required by your software.

1.3 System Requirements

1.3.1 Username Requirements

Only three special characters Hyphen(-), Underscore(_) and period(.) are allowed in username.

Your username can not contain more than one special character.

These checks are done both for the local user and SSO user.

1.3.2 Password Requirements

Your password must meet the following requirements:

- Must be between 8 and 20 characters long.
- Must contain one numeral from 0 to 9.
- Must contain one lowercase letter from a to z.
- Must contain one uppercase letter from A to Z.
- Must contain one of the following special characters: @#\$*!^

1.4 Browser Support

SmartHub INFER™ supports the latest versions of the following browsers:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge

Note: Internet Explorer and Safari browsers are not supported.

1.5 Privacy Notice

INFER™ collects data from IoT and end-user devices as configured by you. When using, you are solely responsible for complying with all applicable laws which include, but not limited to, data privacy laws.

You are responsible for providing any necessary notice, and for obtaining any necessary consents, for the data you collect and send to INFER™. For more information, see [SmartHub's Privacy Policy](#).

1.6 Trademarks

Trademarked names are used throughout this user manual. Rather than put a trademark symbol in every occurrence of a trademarked name, we state that we are using the names only in an editorial fashion and to the benefit of the trademark owner with no intention of infringement of the trademark. All trademarks or service marks are the property of their respective owners.

Copyright © 2025, SmartHub, Inc. All rights reserved.

2 Configuring Your Organization

This chapter covers the concepts and steps to configure Organizations, sub-organizations, Users, Groups, and Roles from INFER™.

You can configure your organization level by providing credentials that were created by the organization Administrator.

Note: System Administrators create and provision organizations, whereas, Organization Administrators manage users, groups and devices. For more information, see [Groups](#).

2.1 Roles and Permissions

Prerequisite: To perform specific operations on the INFER™ Console, you must have the required roles and permissions.

2.1.1 Roles

INFER™ provides the following default roles:

Default Role	Description
Space Administrator	You can add, modify, assign/unassign, and delete spaces to devices in your organization.
Identity and Access Administrator	You can add or modify an organization, add or modify users, groups, roles, and notifications, and view audit logs.
Campaign Administrator	You can add or modify campaigns, packages for OTA updates, and view notification definitions and notification destinations.
Package Administrator	You can add or delete packages.
Device Administrator	You can add or modify devices and asset templates.
Gateway Administrator	You can add devices, create asset tokens and credentials, and view asset templates.
Alert Administrator	You can acknowledge alerts and view alerts, organizations, users, roles, groups, asset, asset templates, notifications, and so on. This is a view only role.
Monitoring Administrator	You can modify alerts and notifications, and view metrics.
Asset ledger Admin	You can create, view and edit Asset related data.
Edit Sensitive Properties	You can create, view and edit a Device's properties that are flagged as sensitive.
Insights Viewer	You can view various Dashboards under the Insights menu.
Insights Editor	You can create, view and edit Dashboards under the Insights menu.
View-Only User	You have only view permissions for everything but cannot modify anything.

The exact list of **Permissions** for each of these **Roles** can be found on INFER™ Console under **Identity & Access > Roles**.

2.1.2 Groups

A group in INFER™ is a set of users who share a common purpose. All members of a role group are assigned the same set of roles.

INFER™ provides the following default **Groups**.

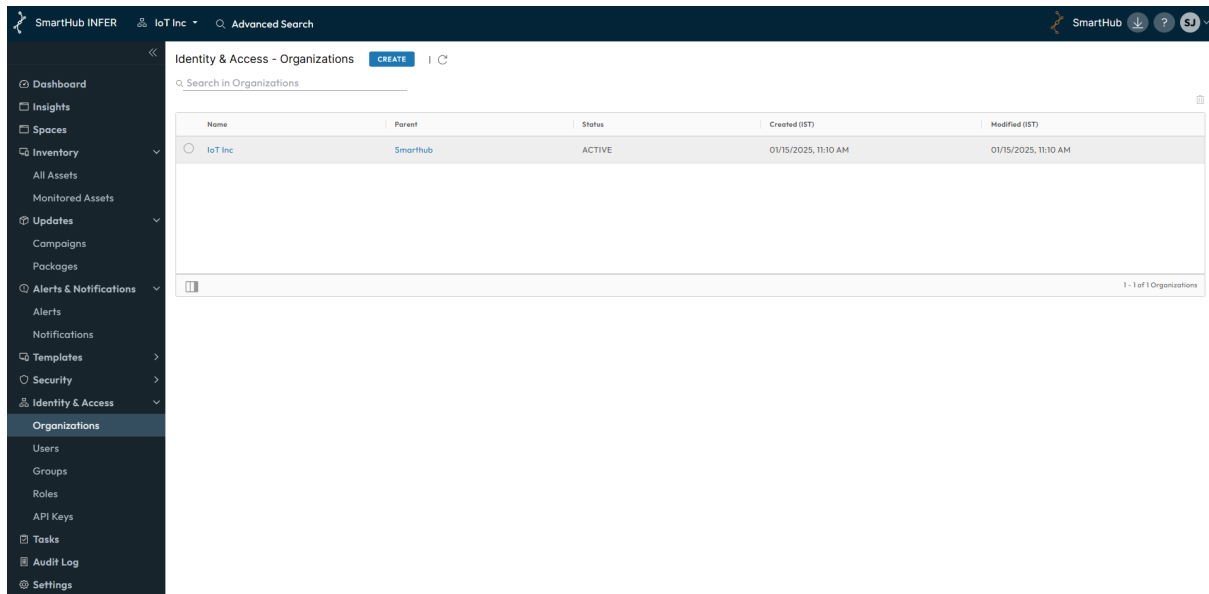
Group	Roles
Organization Administrators System Administrators	Identity and Access Administrator Campaign Administrator Space Administrator View Organization Package Administrator Device Administrator Gateway Administrator Alert Administrator Monitoring Administrator Asset Ledger Administrator Edit Sensitive Properties Insights Viewer
Data Extraction Group	View-Only User

Note: Any user with the **Identity & Access Administrator** role can modify these default roles or create new roles.

2.1.3 Viewing Organization Details

This section lists the steps to view an organization and its details.

Prerequisite: You must have the VIEW_ORGANIZATION permission to perform this operation.



1. On the INFER™ UI, under the **Organizations** page, click an organization.
The Organizations page displays your organizations, and their status as listed below:

Section	Description
Basic Information	Displays details such as the name of the organization, its creation date and time, parent organization if any, and modified date and time.
Users	Displays the list of users under the organization with their display name, status, created date and time, and modified date and time.
Assets	Displays the asset information such as asset type, enrollment status, and the date of creation and modification.
Usage	Displays the usage meter of the various states of alerts, campaigns, devices, organizations, and notifications.

2.1.4 Creating an Organization

This section lists the steps to create an organization on the INFER™ UI.

Prerequisite: You must have the permissions associated with the Organization Administrator role to perform this operation.

1. On the INFER™ UI, navigate to **Identity & Access > Organizations**. The **Organizations** page appears.
2. Click **CREATE**. The **Create Organization** wizard appears.
3. Under **Basic Information**, perform the following steps:
 - a. Enter the name of your **Organization**.
 - b. Select the parent organization from the **Parent Organization** drop-down menu.

Note: The maximum depth to which a sub-organization can be created for an organization is four.

- c. Under **Organization Identifier**, enter a unique identifier name to identify your organization with. If you are a part of multiple organizations, use this identifier when signing in so that INFER™ associates you with the correct organization.

Note: Organization Identifier is not a mandatory field.

- d. Check the **Create Default Roles & Groups** checkbox.
4. Click **Next**.
 5. Under **Review**, review the information you have entered and click **SAVE**. You have successfully created an organization.

2.1.5 Editing an Organization

This section lists the steps to edit an organization from the INFER™ Console.

Prerequisite: You must have the permissions associated with the Organization Administrator role to perform this operation.

1. On the INFER™ UI, navigate to **Identity & Access > Organizations**. The Organizations page appears.
2. Click the organization to edit. The details of the organization appears.
3. From the **Actions** drop-down menu, click **Edit**. The **Edit Organization** window appears.

4. Update your organization details and click **SAVE**.
You have successfully updated your organization details.

2.1.6 View Usage

You can measure the usage of services such as notifications, users, file records, devices, alerts, commands, metrics, alert definitions, campaigns, that are running in your organization. The values appear for the current organization and its sub-organizations.

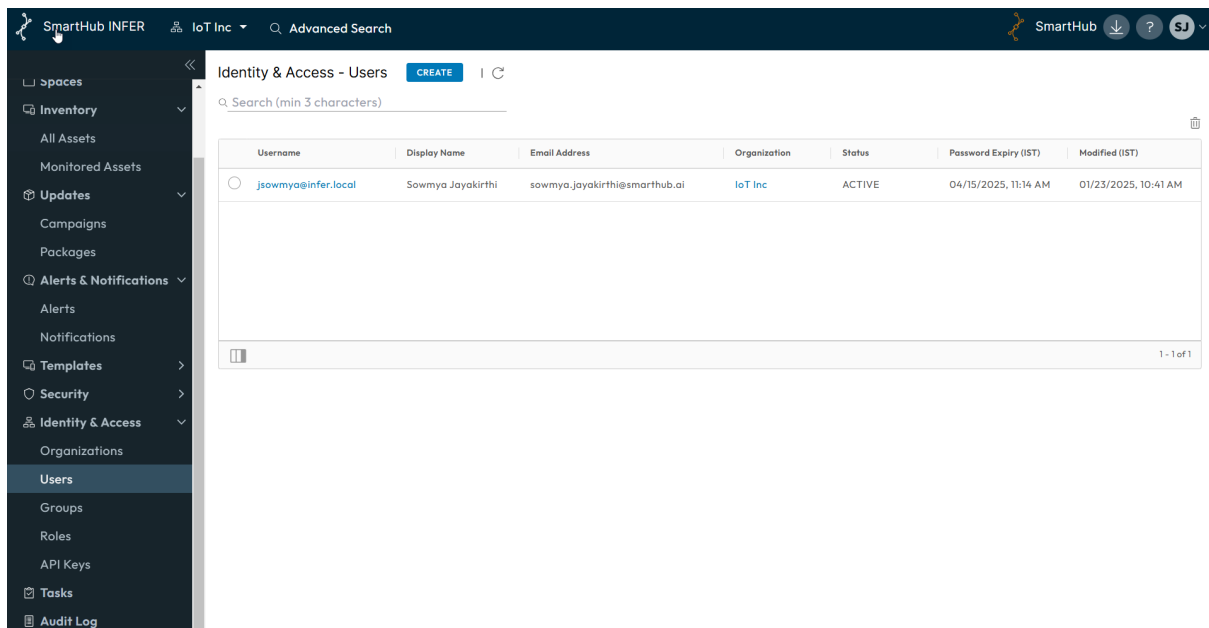
Prerequisite: Verify that you have Identity & Access administrator access to perform this operation.

1. On the INFER™ Console, navigate to **Identity & Access > Organizations** and select your organization.
2. On the organization details page, click the **Usage** tab.
3. To view the usage from the time the organization was created, click **ALL HISTORY**.
4. To view the usage for a particular duration, click **CUSTOM** and select the duration.
5. Click **VIEW DETAILS**.
The services and their usage values appear.
6. To export the usage values in **CSV** format, click **EXPORT AS CSV**.

2.2 Users

INFER™ determines the level of access for the user based on the permissions that you assign to the user.

The permissions defined for these users apply whenever a user connects to INFER™.



2.2.1 Creating a User

This section lists the steps to create a user from the INFER™ Console.

Prerequisite: You must have the CREATE_USER permission to perform this operation.

1. On the INFER™ UI, navigate to **Identity & Access > Users**.
The **Identity & Access - Users** page appears.

2. Click **CREATE**.
The **Create User** wizard appears.
3. Under **Details**, enter the following details:

Section	Description
Display Name	Enter the display name of the user.
Username	Enter the user name to use for logging in to INFER™.
Email Address	Enter a valid email ID.
New Password	Enter a password for the user. For information about password requirements, see "Password Requirements"
Confirm New Password	Confirm the password that you have entered.

4. Click **Next**.
5. Under **Groups**, select the appropriate groups for the user and click **Next**.
6. Under **Review**, review the information and click **SAVE**.
You have successfully created a user.

2.2.2 Editing a User

You can edit a user from the INFER™ Console.

Prerequisite: You must have the EDIT_USER permission to perform this operation.

1. On the INFER™ UI, navigate to **Identity & Access > Users**.
The **Identity & Access - Users** page appears.
2. Click the user to edit.
3. From the **Actions** drop-down menu click **Edit**.
Here, you can update the display name of the user, change the user status, add or delete groups to the user, and add or delete roles.
4. Update your user details and click **SAVE**.
You have successfully edited the user details.

2.2.3 Deleting a User

You can delete a user from the INFER™ UI.

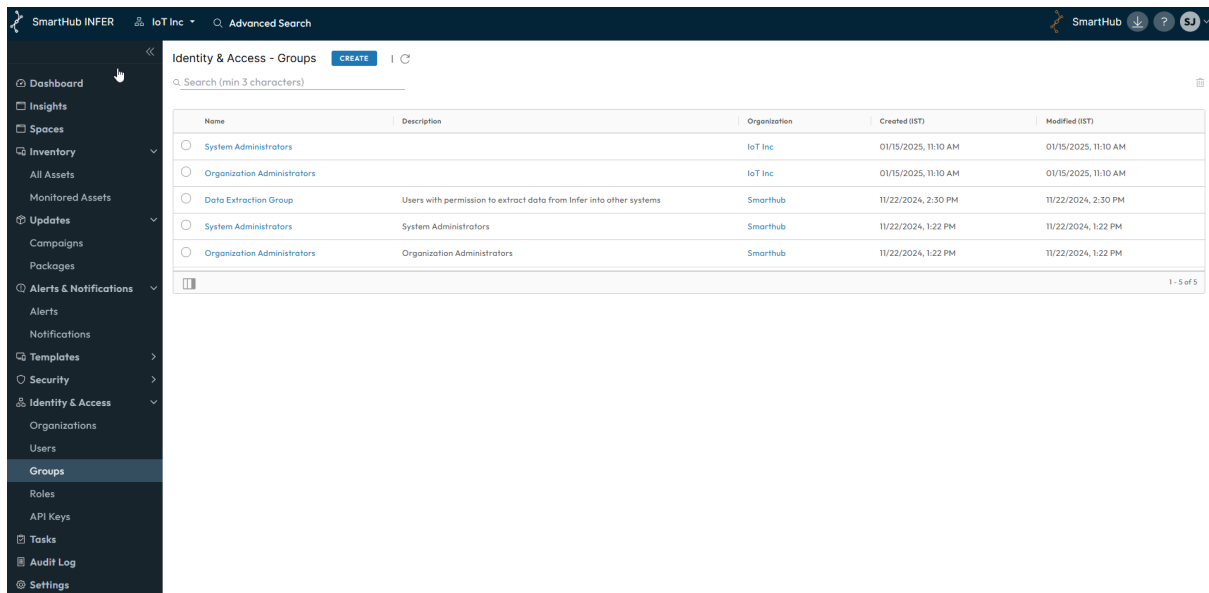
Prerequisite: You must have the DELETE_USER permission to perform this operation.

1. On the INFER™ UI, navigate to **Identity & Access > Users**.
2. Select the user to delete.
3. Click the delete icon on the top-right side of the screen. You can also select **Delete** from the **Actions** drop-down menu.
An action confirmation message appears.
4. To confirm the action, click **DELETE**. You have successfully deleted a user.

2.3 Groups

You can manage a set of users with similar permissions through groups. Using groups can reduce the time it takes to set up your permissions model.

A user can be a member of more than one group. When you assign permissions to a group, all users in the group inherit those permissions.



2.3.1 Creating a Group

This section lists the steps to create a user group from the INFER™ Console.

Prerequisite: You must have the CREATE_GROUP permission to perform this operation.

1. On the INFER™ UI, go to **Identity & Access > Groups**.
The **Identity & Access - Groups** page appears.
2. Click **CREATE**.
The **Create Group** wizard appears.
3. Under **Details**, enter the group name and a short description about the group. Click **NEXT**.
4. Under **Roles**, select a role for the group. Some of the default roles are as follows:
 1. Identity & Access Administrator
 2. Campaign Administrator
 3. Package Administrator
 4. Device Administrator
5. Click **Next**.
6. Under **Review**, review the information and click **CREATE**.
You have successfully created a user group.

2.3.2 Editing a Group

You can edit user details in a group from the INFER™ Console.

Prerequisite: You must have the EDIT_GROUP permission to perform this operation.

1. On the INFER™ UI, navigate to **Identity & Access > Groups**.
The **Identity & Access - Groups** page appears.
2. Click the group to edit.
3. From the **Actions** drop-down menu, click **Edit**.
The **Edit Group** wizard appears.
4. Update the group details and click **SAVE**.
You have successfully updated the group.

2.3.3 Deleting a Group

This section lists the steps to delete a group from the INFER™ Console.

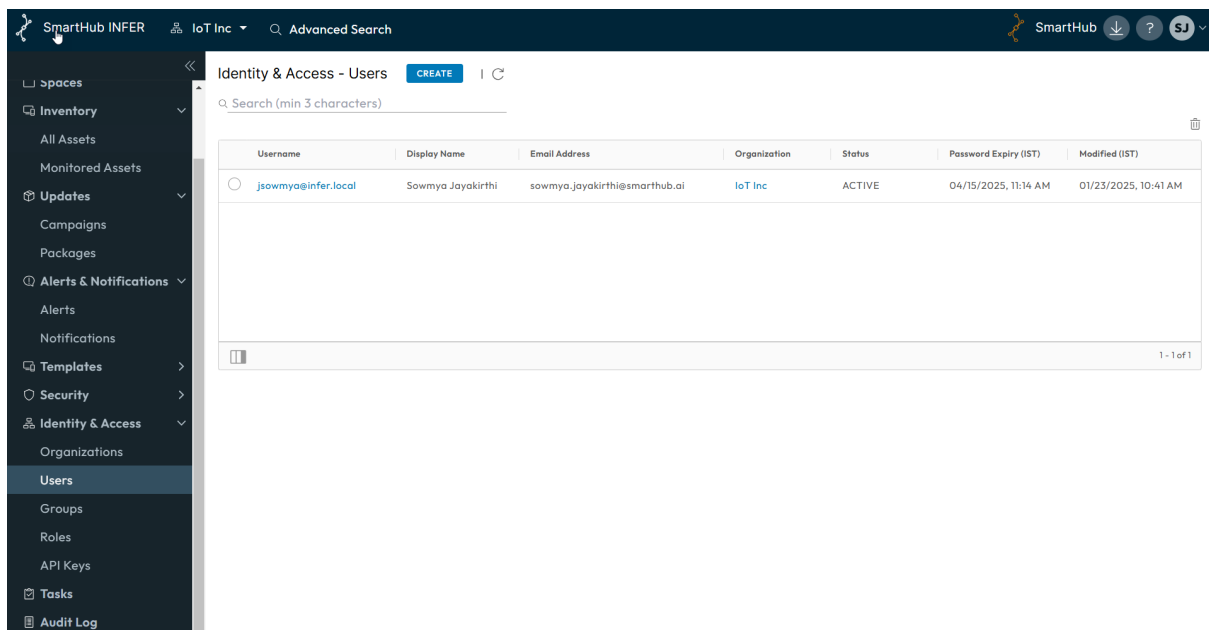
Prerequisite: You must have the DELETE_GROUP permission to perform this operation.

1. On the INFER™ UI, navigate to **Identity & Access > Groups**.
The **Identity & Access - Groups** page appears.
2. Select the radio button against the group to delete.
3. Click the delete icon on the top-right side of the screen. Or, select **Actions > Delete**.
An action confirmation message appears.
4. To confirm the action, click **DELETE**.
You have successfully deleted the group.

Note: This action deletes the group permanently.

2.4 Roles

A role is assigned to a user or a group with a predefined set of privileges. A single user can have different roles.



2.4.1 Creating a Role

This section lists the steps to create a role from the INFER™ Console.

Prerequisite: You must have the CREATE_ROLE permission to perform this operation.

1. On the INFER™ UI, navigate to **Identity & Access > Roles**.
The **Identity & Access - Roles** page appears.
2. Click **CREATE**.
The **Create Role** wizard appears.
3. Under **Details**, enter the role name and a short description about the role. Click **Next**.
4. Under **Permissions**, select the permissions to assign to the role. Click **Next**.
5. Under **Review**, review the information and click **SAVE**.
You have successfully created a role.

2.4.2 Editing a Role

You can edit a role from the INFER™ Console.

Prerequisite: You must have the EDIT_ROLE permission to perform this operation.

1. On the INFER™ UI, navigate to **Identity & Access > Roles**.
The **Identity & Access - Roles** page appears.
2. Click the role to edit.
3. From the **Actions** drop-down menu, click **Edit**.
The **Edit Roles** wizard appears.
4. Update the role details and click **SAVE**.
You have successfully updated a role.

2.4.3 Deleting a Role

You can delete a role from the INFER™ Console.

Prerequisite: You must have the DELETE_ROLE permission to perform this operation.

1. On the INFER™ UI, navigate to **Identity & Access > Roles**.
The **Identity & Access - Roles** page appears.
2. Select the role to delete and click the delete icon on the top-right side of the screen.
Or, select **Actions > Delete**.
An action confirmation message appears.
3. To confirm the action, click **DELETE**.
You have successfully deleted a role.

3 Space Management

This chapter explains space templates, and lists steps to create and edit space templates and assign them to physical spaces.

Space management in INFER™ refers to the use of connected IoT devices, sensors, and actuators to optimize the utilization, efficiency, and overall management of physical spaces, such as buildings, offices, factories, warehouses, parking lots, public areas, and other commercial or residential areas.

3.1 Smart Spaces

Smart spaces refers to environments that are equipped with various IoT devices, sensors, and technologies to collect, analyze, and act on data to optimize efficiency, enhancing user experiences, and improving overall functionality. Such spaces are designed to be intelligent, interconnected, and responsive, utilizing advanced technologies to create more intuitive and seamless interactions between people, devices, and the surrounding environment.

3.2 Use Cases

With IoT-driven space management systems, businesses and organizations can deploy devices and sensors to make their spaces more responsive to the needs of occupants, enhance sustainable security, while also gain real-time insights and control over various aspects of their spaces, leading to increased efficiency, better resource utilization, optimize operational costs and intelligent resource usage.

With IoT devices and sensors driven space management systems, improves efficiency, optimizes resource usage, and enhances user experiences across various domains, from homes and offices to agriculture and retail spaces.

Listed below are some ways spaces can be managed using IoT devices and sensors:

Smart Building Management

- **Occupancy Tracking:** IoT sensors can monitor the occupancy of rooms, desks, or workstations in offices, helping to optimize heating, cooling, and lighting based on real-time occupancy data. This data can be analyzed to optimize space utilization, identify under utilized areas, and facilitate flexible seating arrangements for agile working environments.
- **Environmental Monitoring:** IoT sensors can monitor temperature, humidity, air quality, and lighting levels to ensure optimal comfort and energy efficiency. This data helps ensure optimal working conditions for occupants and can be used to implement air quality improvement measures.
- **Energy Management:** Smart meters and IoT-enabled devices can track energy consumption, enabling better control and optimization of energy usage in buildings.
- **Lighting Control:** IoT-based lighting systems can adjust brightness and switch on/off lights automatically, considering factors like natural light levels and occupancy.
- **Smart HVAC Automation:** IoT sensors and devices can monitor and control various systems, including Heating, Ventilation, and Air Conditioning (HVAC) considering factors like occupancy. The system can adjust settings based on occupancy, weather conditions, and energy demand, leading to significant energy savings and improved occupant comfort.
- **Security and Surveillance:** IoT-enabled cameras and sensors can detect unauthorized access, monitor critical areas, and send real-time alerts to security personnel in case of suspicious activities.

- **Smart Parking Solutions:** IoT sensors in parking lots or on streets can detect available parking spaces in real-time. This information can be communicated to drivers through mobile apps, reducing traffic congestion and helping users find parking spots quickly.
- **Indoor Navigation and Wayfinding:** IoT-enabled beacons and sensors in large buildings, airports, or shopping malls can provide indoor navigation assistance to visitors and customers. Mobile apps can guide users to their desired locations, enhancing customer experience and engagement.
- **Facility Maintenance and Management:** IoT sensors can monitor the health of equipment and infrastructure in buildings and industrial facilities. Predictive maintenance algorithms can detect potential issues, allowing for proactive repairs and minimizing downtime.

Smart Office Spaces

- **Workspace Utilization:** IoT sensors can monitor desk and meeting room occupancy to optimize space utilization and provide insights for facility planning.
- **Environmental Comfort:** Sensors can maintain optimal indoor conditions, such as temperature and air quality, to improve employee comfort and productivity.
- **Energy Efficiency:** Smart office systems can adjust lighting, heating, and cooling based on occupancy and ambient conditions to reduce energy waste.

Smart Retail Spaces

- **Customer Analytics:** IoT sensors can track customer behavior and movements patterns to optimize store layouts and product placements. This data can also be used for targeted marketing and enhancing the overall shopping experience.
- **Inventory Management:** IoT-enabled RFID tags can help retailers track inventory levels and automatically restock items as needed.
- **Smart Waste Management:** IoT sensors in waste bins can monitor fill levels, optimizing waste collection routes, and reducing unnecessary pickups, leading to cost savings and more efficient waste management.

Smart Home Automation

- **Home Security:** IoT devices like cameras, motion detectors, and door/window sensors can enhance security by providing remote monitoring and alert systems.
- **Home Appliances:** IoT-connected appliances allow users to control and monitor their devices remotely, promoting energy efficiency and convenience.
- **Voice-Activated Assistants:** Smart speakers and virtual assistants like Amazon Echo or Google Home can manage home devices and provide information or perform tasks via voice commands.

Smart Agriculture

- **Smart Farming:** IoT sensors in agriculture can monitor soil moisture, temperature, and nutrient levels, enabling precise irrigation and fertilization practices.
- **Livestock Monitoring:** IoT devices can track the health and behavior of animals, providing valuable data for improved livestock management.
- **Crop Monitoring:** Drones and IoT sensors can assess crop health, growth, and pest infestations, facilitating timely interventions for higher yields.

3.3 Create a Space Template

A space template in INFER™ is the blue print of the spaces where the attributes provide additional info to qualify the spaces. The space template sources its attributes from your

space management application as per the defined data model and configurations to stay connected.

Prerequisite: You must have the `CREATE_SPACE_TEMPLATE` permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ UI, navigate to **Templates > Spaces**. The **Templates - Spaces** page appears.
2. Click **CREATE**. The **Create Space Template** wizard appears.
3. Under **Space Template Name**, enter the desired template name.
4. Under **Description**, enter a brief description of the space template you are creating.
5. Click **NEXT**.
6. Under **Attributes**, under **Name**, enter the attribute's name.
7. Under **Type**, from the drop-down menu, choose the desired attribute type.

Note:

- If you choose **STRING**, you can enter an optional value that will appear as the default value while creating a space.
- If you choose **CONSTANTS**, you can enter multiple comma separated values (CSV) that will appear together as a drop-down menu while creating a space.

Create Space Template

- 1 Detail
- 2 Attributes
- 3 Review

Attributes

Space Template Attributes

Name	Type	Value	
Conference Room	STRING	3000	
Max_Occupancy_Threshold	CONSTANTS	20, 30, 30	

[+ Add](#)

[CANCEL](#)
[BACK](#)
[NEXT](#)

8. Click **NEXT**.
9. Under **Review**, review the space template information you entered and click **SAVE**. You have successfully created a space template.

You can now view your space template in the **Inventory - Space Templates** page as shown below:

Space Template Name	Description	Parent Templates	Organization	Created	Modified
BLR Meeting	Meeting rooms	-	SmartHub	02/07/2025, 1:07 PM	02/07/2025, 1:07 PM
Campus	Campus	-	SmartHub	01/05/2024, 1:39 PM	09/05/2024, 3:04 PM
Reception Area	Reception area of the floor or building	Floor, Canteen Area	Safe Spaces Inc.	05/16/2023, 1:57 PM	12/12/2023, 8:35 AM
Canteen Area	Canteen area of a building or a floor	Floor	Safe Spaces Inc.	05/16/2023, 1:58 PM	05/16/2023, 1:59 PM
Room	Room name or number	Floor	Safe Spaces Inc.	05/16/2023, 1:55 PM	05/16/2023, 1:59 PM
Floor	Floor number or name in the building	Building	Safe Spaces Inc.	05/16/2023, 1:53 PM	05/16/2023, 1:59 PM
Building	Name of the Building	City	Safe Spaces Inc.	05/16/2023, 1:51 PM	05/16/2023, 1:59 PM
City	Name of the city	Country	Safe Spaces Inc.	05/16/2023, 1:48 PM	05/16/2023, 1:59 PM
Country	Name of the country	-	Safe Spaces Inc.	05/16/2023, 1:47 PM	05/16/2023, 1:47 PM

3.4 Editing a Space Template

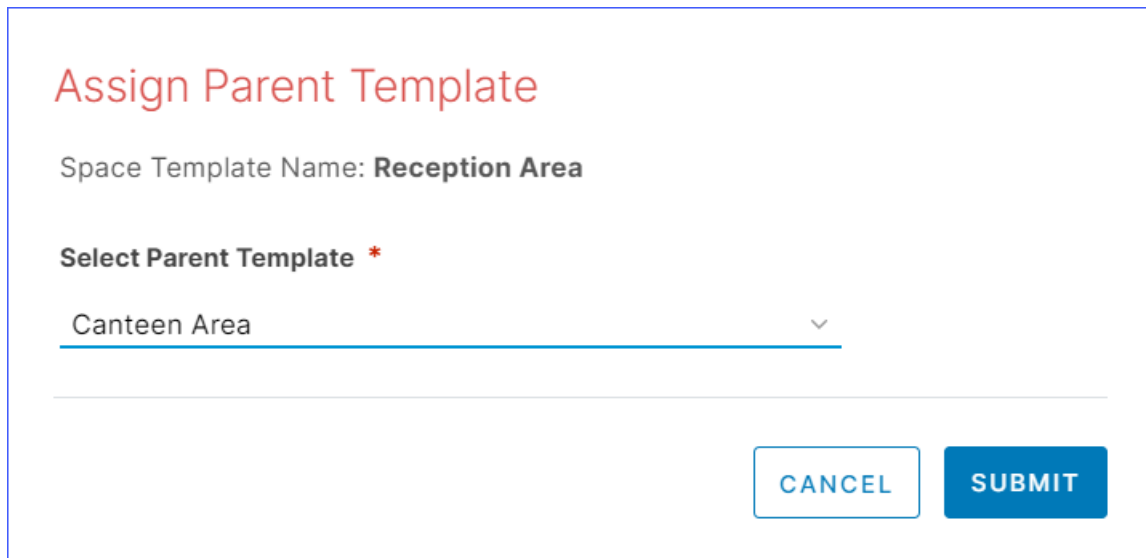
Prerequisite: To edit an existing space template in INFER™, you must have the EDIT_SPACE_TEMPLATE permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ UI, go to **Templates > Spaces**. The **Inventory - Space Templates** page appears.
2. From the listed templates, click the template you desire to edit.
3. Under **Actions**, from the drop-down menu, click **Edit**.
4. The **Update Space Template** wizard appears. Here, update the **Display Name**, **Space Attributes** and click **NEXT**.
5. Under **Review**, review the information and click **SAVE**. You have successfully edited a space template.

3.5 Assigning a Parent Template

Prerequisite: To assign a parent template in INFER™, you must have the EDIT_SPACE_TEMPLATE permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ UI, go to **Space Templates**. The **Inventory - Space Templates** page appears.
2. From the listed templates, click the template you desire to assign a parent template.
3. Click the **Parent Templates** tab.
4. On the page's right side, click **ASSIGN PARENT TEMPLATE**. The **Assign Parent Template** pop-up appears as shown below:

A dialog box titled "Assign Parent Template" in red text. Below the title, it says "Space Template Name: Reception Area". Then, there is a label "Select Parent Template *" followed by a dropdown menu. The dropdown menu currently shows "Canteen Area" with a downward arrow. At the bottom right of the dialog box are two buttons: "CANCEL" and "SUBMIT".

Assign Parent Template

Space Template Name: **Reception Area**

Select Parent Template *

Canteen Area

CANCEL SUBMIT

5. Under **Select Parent Template**, use the drop-down menu to select your desired parent template.
6. Click **SUBMIT**. You have successfully assigned a parent template.

3.6 Cloning a Space Template

Cloning a space template involves creating a copy of an existing template to use as a basis for new deployments.

Cloning a space template offers several advantages, especially when setting up multiple IoT projects or deployments with similar configurations. Listed below are some of the key advantages:

- **Consistency:** Cloning a space template ensures a consistent configuration across multiple IoT spaces or projects. This is essential when you need uniformity in device types, data streams, rules, and other settings. It helps reduce the risk of configuration errors and ensures that all instances of the template follow the same standards.
- **Faster Deployment:** Creating an IoT space template with the desired configuration can be time-consuming. When you need to deploy new IoT spaces quickly, cloning a template streamlines the process. You can duplicate an existing, functioning setup, saving valuable time during deployment. You can reuse the existing template as a starting point, sparing you from recreating everything from scratch.
- **Reduced Complexity:** IoT deployments often involve complex configurations with various devices, sensors, and data streams. Cloning a space template simplifies the process by allowing you to copy an existing, working configuration and then make minor adjustments or customizations as needed.
- **Scalability:** As your IoT initiatives grow, it's essential to have a scalable approach. Cloning templates makes it easy to scale your projects efficiently. You can replicate the same configuration for additional spaces, reducing the complexity of managing multiple, distinct setups.
- **Error Reduction:** Creating new IoT configurations manually increases the likelihood of errors, inconsistencies, and omissions. Cloning a template minimizes these risks because the initial configuration is already validated and tested.
- **Standardization:** Cloning templates enables standardization across your IoT deployments. This is crucial for ensuring that best practices, security policies, and compliance requirements are consistently applied across all spaces.

- **Maintenance Efficiency:** When updates or changes are necessary, managing multiple IoT spaces based on a cloned template is more efficient than dealing with disparate configurations. You can make changes to the template and then propagate those changes across all cloned instances.
- **Cost Efficiency:** By reducing the time and effort required for setup and maintenance, cloning templates can lead to cost savings in terms of labor and operational expenses.

Prerequisite: To clone an existing space template in INFER™, you must have the `EDIT_SPACE_TEMPLATE` permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ UI, navigate to **Spaces > Inventory - Spaces**.
2. From the listed templates, click the template you want to edit.
3. Under **Actions**, click **Clone**. The **Create Space Template** wizard appears.
4. Under **Space Template Name**, enter the required details.
5. Under **Description**, enter a brief description of the new template and click **NEXT**.
6. Under **Attributes**, modify the cloned space template's attributes. Click **+ Add** icon to add new attributes, and click **NEXT**.
7. Under **Review**, review the information and click **SAVE**. You have successfully cloned a space template.

3.7 Deleting a Space Template

Prerequisite: To delete an existing space template in INFER™, you must have the `DELETE_SPACE_TEMPLATE` permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ UI, navigate to **Spaces > Inventory - Spaces**.
2. From the listed templates, click the template you desire to edit.
3. Under **Actions**, click **Delete**.
4. The **Delete Space Template** pop-up appears as shown below:

Delete Space Template

Are you sure you want to delete the Space Template(s) listed below?
This action is permanent and cannot be recovered.

Enter **DELETE** below to confirm action*

DELETE

Space Template Name: **Reception Area**

CANCEL
DELETE

5. Enter **DELETE** in the text area, and click **DELETE**. You have successfully deleted a space template.

Note: If the selected space template is already associated with a child space, deletion will not occur.

4 Working with an Asset as a Template

This chapter explains assets, asset as a template, and the steps to create and edit asset and asset templates.

An asset template takes stock of the device's behaviors and actions by collecting system properties from an asset, metrics, and detects supported device commands as per the defined data model.

It serves as a predefined structure or blueprint that defines the characteristics, functionalities, and behaviors for multiple asset with similar features and configurations to stay connected.

Note: SmartHub INFER™ has updated its navigation elements in the user interface. The user guide has renamed the following UI elements and the respective navigation steps have also modified:

1. The **Devices** tab has been renamed **Monitored Assets**.
2. The **Asset Ledger** tab has been renamed **All Assets**
3. **Spaces** is a new tab in the INFER™ UI.
4. **Alerts & Notifications** now lists **Alerts** and **Notifications** as separate elements.
5. The **Templates** tab lists **Assets**, **Alerts**, **Notifications**, and **Spaces** as separate elements.

4.1 What is an Asset?

An asset in INFER™ refers to an entity which can be given an identity, be managed, which stays connected to the internet and is capable of collecting, transmitting, and receiving data. Such assets come with sensors, software, and network connectivity, allowing them to interact with their surroundings, other assets, and users.

There are 2 types of asset:

1. **Gateway:** An asset entity in which an Agent can be run directly, giving you greater control and which also allows you to talk to other assets connected directly, one hop away or multiple hops away using wireless, wired, blue-tooth, or any other IoT protocol, forming a multi-layered model similar to a tree of assets.

N number of Things can be connected to a gateway. A gateway remains thing agnostic as long as it is explicitly stated that this gateway type supports the respective types of sensors and things. For more information, see [What is a Gateway?](#)

Note: A gateway in INFER™ is designed to support a maximum of 400 assets, configured as a soft limit.

2. **Thing:** A very light weight asset entity without a microprocessor, in which an Agent cannot be run directly. Here, the agent is installed in a separate hardware or virtual hardware i.e. a virtual machine or a container.

Here, the entire INFER™ platform enables the execution of any action on the Console by ensuring that the command reaches the gateway, to the agent, from the agent to the right adapter and the adapter knows how to transfer that command to that asset, wait for the outcome of the command, and take it back to the user who gave that command.

Note: Besides being Console driven, this can also be done using a REST API.

This way INFER™ supports a multi-tiered tree of individual IoT assets with complex relationships that can be modeled and managed.

4.2 What is an Asset Template?

When we consider IoT assets in an enterprise, it is in scale amounting to hundreds of thousands of assets. It is practically impossible to deal with each asset one at a time. This

situation therefore calls for an ability to deal with thousands of assets at a time. To do so, INFER™ provides a generic model which we call an **Assets**.

The assets in INFER™ is a **JSON** file that serves as a asset's or asset groups' blueprint needed by their adapters residing in INFER™. The asset template takes stock of the asset's behaviors and actions by collecting system properties from the asset, metrics, and detects the commands supported by the asset as per the defined data model.

There are two types of templates in INFER™:

1. Gateway template type
2. Thing template type

4.3 What are Asset Properties?

The asset template contains the following properties:

- System Properties
- Custom Properties

4.3.1 System Properties

These are the asset properties collected automatically by the Agent. It includes asset data which do not change often like its serial number, firmware version etc. in boolean and string data types.

These properties can also be sent to the INFER™ Server by the User client node of the Agent from the asset itself. You can query these properties using **Advanced Search**.

4.3.2 Custom Properties

Set at the Server side, custom properties are set in free form, are extensible, and are assigned by the administrator for better management of the asset. These properties can be associated with a asset's golden configuration template settings, or warranty information. By default, every new assets gets this data.

Once onboarded, every asset has its own lifecycle where its values, properties and metrics keep changing. These properties can be used for querying information or for sending configuration files to assets.

Driven by APIs/JSONs, all assets have the same structure which a template accomplishes. Custom properties can carry any number of name/value pairs depending on domain, context and other asset information.

The asset template carries commands which specify actions supported by the asset. Connected templates express the relationship between gateway template and Programmable Logic Controller (PLC). The structure is well defined and managed.

4.4 What are Metrics?

Both **Gateway** and **Thing** templates support the Agent's collection of Metrics or telemetry data from the assets specified by the INFER™ server. This numeric, boolean, and string data types are also called time-series data as its values change very frequently.

You can configure metric keys such as **Name**, **Value Type**, and **Display Unit**. The metric value type is pre-defined in the assets and is validated on the Agent.

4.5 INFER™ Agent Daemon

The INFER™ Agent is a gateway container or a virtual machine that allows its adapters to talk to the assets with the INFER™ Server acting as a bridge or conduit using a structured way of APIs.

Agent is the entity which talks back to the INFER™ Server running inside a gateway, and the gateway connects to a thing, the thing connects to more things and so on... The Adapter running in the Agent talks to the asset in its own language to make things work.

Whether the assets are on IP, Modbus, Lonworks, or BACnet, their adapters talk to them, collect data or run commands.

The **Agent Daemon** is a 6MB binary written in C, C++, or Python that has least number of dependencies, can run on any flavor of Linux, Windows, Intel and ARM, 32 bit or 64 bit and on some custom Linux kernels too. It is downloaded from the INFER™ Server with admin privileges and installed to run in the background as a daemon.

Once installed, the daemon talks to the INFER™ Server only as an outbound https (port:443) connection, as there is no inbound need for the Server to get into the agent. As the edge gateway is usually kept in a customer's premises, their firewalls only allow outbound https (port:443) connections, yet also disallow any inbound traffic.

In production, there's one agent daemon for each adapter running in the background, and there are other daemons for each type of adapter. For example, if there is a need to talk to datnet, a datnet adapter is developed. It embeds this SDK which comes packaged with the agent and talks on a local socket to the agent, taking commands from the Server through this agent. This gets all the data into the Server having a rich REST API.

4.6 What is an Adapter?

The adapter is the software piece that bridges the protocol gaps between the asset and the Server. The adapter and asset template work together as tightly coupled entities. If the asset template is revised, the adapter too has to be revised for seamless operation. This way the implementation is in the adapter but the definition is in the asset template.

4.7 Connected Asset Templates

You can configure the type of Thing templates that are allowed to connect to the gateway or to a Thing asset.

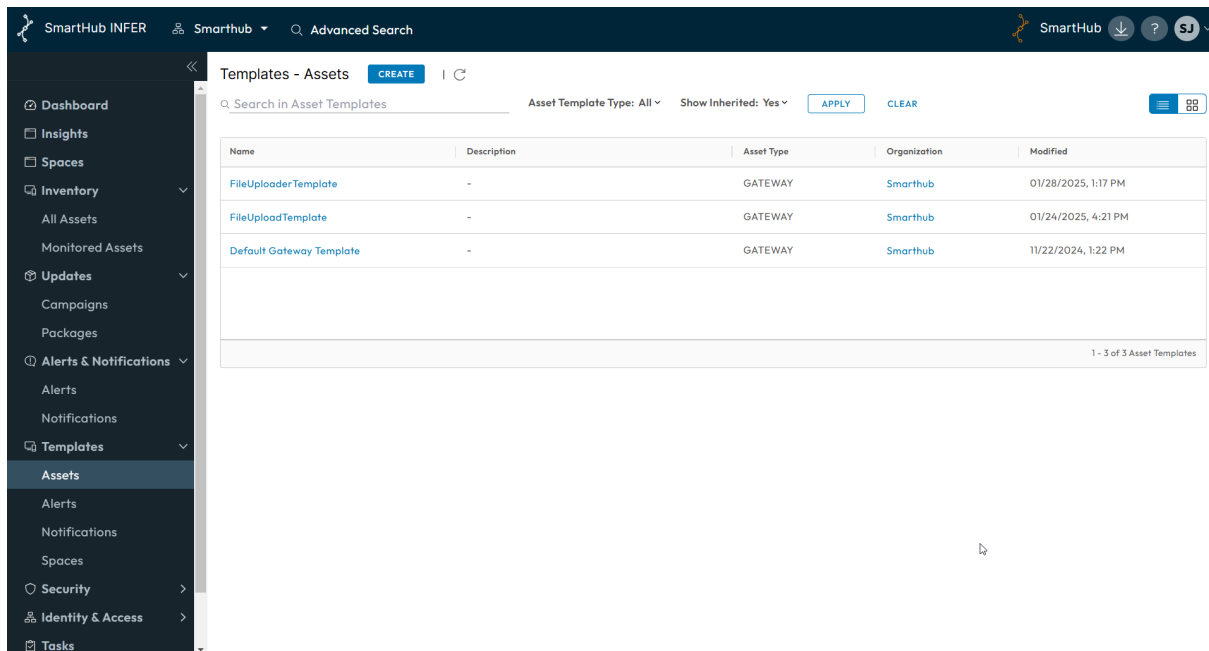
4.7.1 Commands

You can configure the list of commands to send to the gateway. The supported commands are:

1. Client Command
2. Custom Command
3. File Upload
4. Reboot
5. SSH

An asset created from a template receives the default configuration of the template. The asset template helps in creating a simplified process for registering new assets.

An asset can have a restricted list of Thing assets with a specified template. You can create an asset based on the list of available Thing templates. To connect a Thing asset, ensure that the Thing template is a part of the parent gateway template.



To view more details of an asset template, click the name of the desired asset template in the Asset Templates page as shown above.

4.8 Creating an Asset Template

Prerequisite: To create a new asset in INFER™, you must have the `CREATE_DEVICE_TEMPLATE` permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ UI, navigate to **Templates > Assets**. The **Templates - Assets** page appears.
2. Click **CREATE**. The **Create Asset Template** wizard appears.
3. Under **Template JSON**, click **IMPORT** to upload a valid JSON template file.
4. Under **Template Name**, enter the desired template name.
5. Under **Select Asset Type**, choose between **Gateway** and **Thing** from the drop-down menu. If you select a Thing as your asset type then you have an option to toggle the **Is Monitorable** option to change the status of an asset from Deployed to Registered. The *Is Monitorable* key determines whether the assets created from a template will be classified as IoT or non-IoT. If *Is Monitorable* is set to true, it means the assets generated from this template will be IoT devices. As a result, the Infer system can collect metrics, monitor them, and generate alerts accordingly.
6. Under **Description**, enter a brief description of the asset template you are creating.
7. Under **Select Image**, upload a valid image (**JPEG** , **PNG** , or other such formats) that is lesser than 500 KB.
8. Click **NEXT**.
9. Under **Properties**, view the registered asset's system properties that are automatically collected by the Agent or its User client node and sent to the INFER™ Server.

Note: The default system properties appear pre-populated and cannot be deleted.

11. Toggle the **Sensitive** switch for adding an extra layer of protection to a property, and click **DONE**.
12. Click **Add+**, enter a Name and Description, click **Done**.

13. Click the **Edit** icon to modify property parameters like the **Name**, and **Description**.
14. Click **CANCEL** to discard property modifications.
15. Click the **Delete** icon to delete the property.
16. To add a new system property, scroll down and click **+ Add**. Enter the parameters and click **DONE**.
17. Next, scroll down to view **Custom Properties**.

Entered by the administrator, **Custom Properties** are the default properties associated with all the assets attached to this template. These properties are used for querying information or for sending configuration files to the assets. However, unlike **System Properties**, these properties are not collected from the asset and can be edited on the Server.

18. To add a new custom property, scroll down and click **+ Add**. Enter the parameters and click **DONE**.
19. Click **NEXT**.
20. Under **Metrics**, to add more metrics, click **+ Add** and enter the **Display Name**, **Value Type**, **Unit** ensure that the unit is the same as the one collected from the asset and **Description**. If you select **Gateway** as your asset, the **CPU-Usage**, **Memory-Usage**, and **Disk-Usage** metrics appear added by default.

Note: The Metric **Name** and **Value Type** collected from the asset must match the **Metrics** configuration. Else, the configuration will be rejected.

The default metrics are pre-populated. You can delete or add new metrics as required. If you have selected **Gateway** as your asset, perform the next steps. However, if you have selected **Thing** as your asset, go to the last step.

21. Click **NEXT**.
22. Under the **Certificate Signing Request** tab, perform the following steps:
 1. Enter the **CSR Template Name**.
 2. Select the **Bits** from the drop-down menu.
 3. Enter a Description and select the respective Space template under the **Country**, **Country Attribute**, **State**, **State Attribute**, **Locality**, **Locality Attribute** drop-down menus.
 4. Enter an appropriate **Organization Name**, and **Organization Unit**.
 5. Select the Custom Property for the **Common Name**.
 6. Select the IP Address for the Custom Property and click **Add**.
 7. Select the DNS for the Custom Property and click **Add**.
 8. Click **Next**.
23. Under **Connected Asset Templates**, you can edit or delete the thing asset template that is connected to this asset.

Note: Only those assets that belong to the connected templates list can be associated with this asset template.

4.8.1 Adding a Command

1. Under **Commands**, to add a command, click **+ Add**.
2. Under **Type** from the drop-down menu, select the command type you want to run on your asset:

1. **Client Command** - Set a command to communicate with the connected assets in your gateway. For example, you can set a command to turn on the LED that is connected to the gateway when an alert is raised. As a system administrator, you can set a list of allowed client identifiers to be used by the client application when initializing a session with the INFER™ Agent. Ensure that the client identifier you enter matches the client identifier value in the operating system. You can add a client command for both gateway and thing assets.
2. **Custom Command** - Set a custom command. For example, set a command to configure the IP address of the asset or enable DHCP.
 - You must enter the full path of the command. For example, enter `/usr/bin/cp` instead of `cp`.
 - You can add multiple comma-separated arguments for a command.
3. **File Upload** - Set a command to upload log files to the agent. The File Upload command takes multiple file paths in one argument. The Agent archives the files and uploads them to the INFER™ Server as a `.zip` file. Administrators can download the `.zip` file and extract its content.
4. **Reboot** - Set a command to reboot the asset.
5. **SSH** - Set a command to enable or disable SSH on the asset.
3. Under **Description**, enter a brief description of the command you are creating, and click **DONE**.
4. Click **NEXT**.
5. Under **Enrollment Provider**, configure the enrollment provider settings used for creating asset credentials. These credentials are used for onboarding assets securely.
6. Under **Provider Type**, select the desired enrollment provider from the drop-down menu. This creates a single use asset credential with signature and expiry time verification.
7. Under **Provider Config > Identity Key**, specify the key whose value will be presented by this asset during onboarding. Provide an Expiry time in terms of Days, Hours or Minutes.
8. Click **NEXT**.
9. Under **Settings > Allowed Files and File Types**, enter the file name or file type. Click **Add** to select the file.
10. Under **Agent Settings**,
 1. Under **Log Level**, use the drop-down menu to set the logging level for collecting **Error**, **Warning**, **Info** or **Debug** Agent logs on an asset.
 2. Under **Maximum Number of Clients**, set the maximum number of SDK clients that can communicate through the Agent with the INFER™ Server.
 3. Under **Command Fetch Interval (seconds)**, set the periodic interval of polling by the INFER™ Agent to fetch commands from the INFER™ Server. The “0” value indicates an on-demand fetch from Server.
 - The maximum value for the command fetch interval is 43200 seconds. The minimum value is 10 seconds and the default value for the command fetch interval is 30 seconds. If the time interval is not within the specified range, an error message appears.
 4. Under **Metrics Interval (seconds)**, set the time interval between 60 and 43200 seconds for transmitting metrics from the Agent to the INFER™ Server.

Note: The minimum value for the timeout is 60 seconds and the default value for the timeout is 300 seconds. If the time interval is not within the specified range, an error message appears.

5. Under **Server Request Timeout (seconds)**, set the timeout value between 60 and 3600 seconds for requests from Agent to INFER™ Server.

Note: The minimum value for the timeout is 60 seconds and the default value for the timeout is 300 seconds. If the time interval is not within the specified range, an error message appears.

6. Under Network Bandwidth (bytes / second), set the maximum network bandwidth allowed on the asset for the Agent. The data rate is in Bytes per second (B/s). The “0” value indicates unlimited network bandwidth. Configure the network bandwidth cap on the asset for the Agent (in bytes per second).
7. Under **Forward Proxy**, click to enter the Server, Port and user credentials, and click **NEXT**.
11. Under **Network Bandwidth (bytes / second)**, set the maximum network bandwidth allowed on the asset for the Agent. The data rate is in Bytes per second (B/s). The “0” value indicates unlimited network bandwidth. Configure the network bandwidth cap on the asset for the Agent (in bytes per second).
12. Under **Forward Proxy**, click to enter the **Server, Port** and user credentials, and click **NEXT**.

Note:

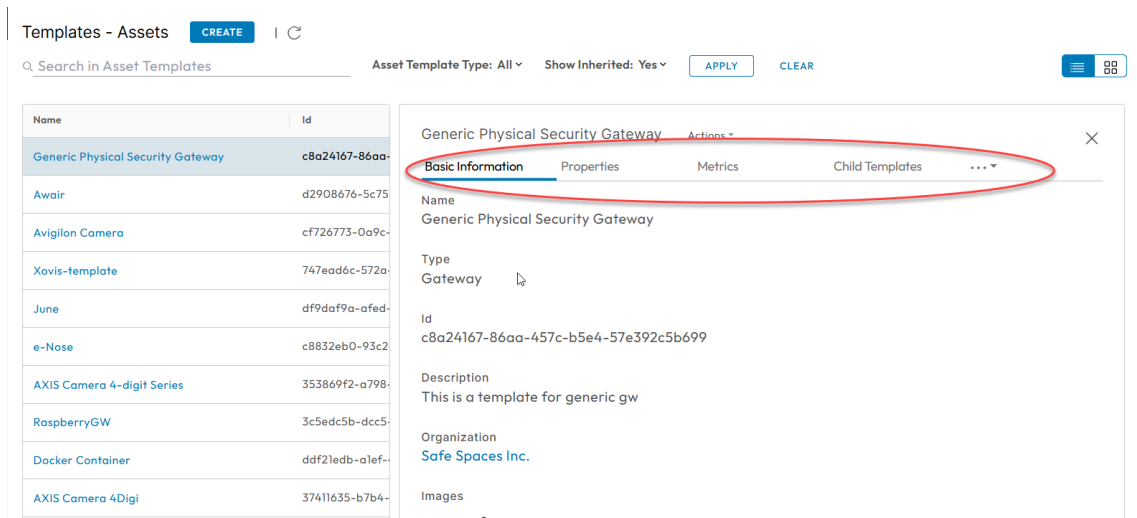
1. You can add multiple HTTP Proxy settings. These proxy settings details are stored in the INFER™ Agent configuration file. The INFER™ Agent uses these proxy settings to connect to the Server for enrolling a gateway.
2. The proxy settings details are then sent to the gateway while enrolling an asset or every time the template is modified. The INFER™ Agent selects the first working proxy Server from the list of proxy servers and updates the same in the INFER™ Agent configuration file.
3. If the current proxy Server stops working, it fetches the next working proxy Server. For enrollment, if the INFER™ Agent cannot connect to the INFER™ Server without connecting to the proxy Server, then you must manually enter the working proxy Server details in the INFER™ Agent configuration file.
4. Under **Review**, review the asset template information you entered and click **SAVE**. You have successfully created an asset template.

You can now view your asset template in the **Inventory - Monitored Assets** page.

4.9 Editing an Asset Template

Prerequisite: To edit an existing asset template in INFER™, you must have the EDIT_DEVICE_TEMPLATE permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ UI, navigate to **Templates > Assets**.
2. From the listed templates, click the template you desire to edit. The following tabs appear as highlighted below:



3. Select the asset template that you want to edit.
4. From the **Actions** drop-down menu, click **Edit**. The **Edit Asset Template** wizard appears. Here, you can edit the system properties, custom properties, add metrics, add a connected asset template, and add commands.

Note: You cannot edit the template name and asset type.
5. Under **System Properties**, click the **Edit** icon against a property to edit that property, make required changes and click **DONE**.

Note: If this asset template is revised, you must ensure that its corresponding adapter too is revised to continue to work together with this template.
6. To delete a property, click the **Delete** icon.
7. To add a new system property, click **+ Add** and enter the property name, and click **DONE**.
8. Under **Review**, review the asset template information you entered and click **SAVE**. You have successfully edited an asset template.

4.10 Adding a Child Template

Prerequisite: To edit an existing asset template in INFER™, you must have the EDIT_DEVICE_TEMPLATE permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ UI, navigate to **Templates > Assets**.
2. Click **Child Templates** tab.
3. Click **Edit**.
4. Under **Edit Allowed Asset Templates** window, click **+ Add**, select the Template from the drop-down menu.
5. Click **Done**.
6. Click **Save**

Note: You can add a Thing to a sub-org but you cannot add as child template to a main organization.

4.10.1 Redirecting an Output Using Custom Commands

This section gives an example to redirect outputs using INFER™'s Custom Command feature.

You can run a script or a binary on a gateway and redirect its output to a file. You can then retrieve the output file using the **Upload** command.

In this example, we run a ping on a gateway to detect its connectivity to a certain end-point. To perform this operation, you must wrap the command into a shell by providing the `/bin/sh` path as the executable, and pass the actual binary and arguments to the shell.

Then, you must pass the `-c` argument to interpret the rest of the arguments as binary and associate the arguments to the binary. Perform the following steps:

1. In the **Create Asset Template** wizard, proceed to the **Commands** page.
2. Under **Commands**, click **+ Add**.
3. Under **Type**, select **Custom Command** from the drop-down menu.
4. Under **Description**, enter a brief description.
5. Under **Name**, enter a name.
6. Under **Executable**, enter the complete path of the executable, for example: `usr/bin/\<executable_name\>` .
7. Under **Arguments**, click **+ Add**.
8. Under **Name**, enter a name.
9. Under **Value**, enter comma to separate multiple values and click **DONE**.
10. Check **Run with root privilege** if you desire to run this custom command.
11. Click **NEXT**. The output for `ping -c 4 8.8.8.8` is redirected to the `ping.txt` file.

5 Onboarding Gateways

This chapter explains the concepts and steps to onboard and configure your gateway in to the INFER™ platform.

5.1 What is a Gateway?

An gateway is an asset or software component that serves as a conduit between IoT assets and the INFER™ platform. Its primary function is to enable communication, data transmission, and coordination between IoT assets and INFER™.

Listed below are the functions of a gateway:

- **Protocol Translation** Gateway assets use a variety of communication protocols, such as MQTT, CoAP, Zigbee, Bluetooth, Wi-Fi, Z-Wave, or proprietary protocols. Gateways are equipped to translate these protocols into a common format to ensure seamless communication between assets and INFER™.
- **Connectivity Management:** Gateways maintain the connectivity between IoT assets and server. They handle tasks like asset registration, authentication, and network configuration, ensuring reliable and secure communication.
- **Data Aggregation and Pre-processing:** Gateways collect data from multiple assets within their range or network. They can perform basic data pre-processing tasks like filtering, aggregation, and compression before transmitting the data to INFER™. This helps reduce network congestion and optimize data transmission.
- **Local Processing and Edge computing:** Certain gateways are equipped with processing capabilities to perform data analysis and run local applications or algorithms. This enables real-time decision-making at the edge of the network, reducing latency and dependency on cloud resources.
- **Security and Data Privacy:** Gateways play a crucial role in ensuring the security and privacy of Edge systems. They can enforce security policies, encrypt data, and authenticate assets before allowing data transmission to the central server or cloud.
- **Asset Management and Firmware Updates:** Gateways facilitate asset management tasks, including remote configuration, monitoring, and firmware updates. They provide a centralized control point for managing a fleet of IoT assets, ensuring their proper functioning and updating their software when necessary.
- **Integration with Cloud and Backend Systems:** Gateways establish a connection between things and the INFER™ platform. They transmit the collected data to the cloud for further processing, analysis, storage, and visualization. They also enable bi-directional communication, allowing commands or control signals from the cloud to reach the assets.

To begin with, you need a asset template to represent a gateway. An asset template serves as a predefined structure or blueprint that defines the characteristics, functionalities, and behaviors for multiple assets with similar features and configurations to stay connected.

Note: The definition is in the template, and its implementation is done in the adapter. Therefore, if the asset template is revised, the adapter too has to be revised to work together with the template.

To on-board your gateway, perform the following steps:

1. Create an asset template as explained in [Creating an Asset Template](#).
2. Download and install the Agent as explained in [Installing INFER™ Agent](#).
3. Onboard your gateway using one of the following authentication protocols:
 1. **Basic Authentication:** The administrator uses his own credentials to enroll the gateway. A simple authentication scheme built into the HTTP protocol. The

client sends HTTP requests with the Authorization header that contains the word `Basic` followed by a space and a base64-encoded string `username:password`.

2. **Token-based Authentication:** A single use gateway credential with signature and expire time verification token is generated on the Server. This token is used by the administrator who's installing the agent on the edge to enroll. This token is then manually transferred to the asset which claims this token as its identity, very similar to the OTP used in mobile authentications.
3. **Property-based Authentication:** To bulk enroll hundreds of agents, a hardware box with a CPU is identified, and its unique asset identity value such as its MAC address or its IP address is used as a single use gateway credential to authenticate bulk enrollment of gateways.
4. **TPM-based Authentication:** The administrator creates a single use gateway credential with a Trusted Platform Module (TPM) identity value verification. Using this authentication method, you can whitelist a gateway so that it is allowed for enrollment.

The Trusted Platform Module (TPM) is built into the CPU to store confidential information. Some semi-conductor companies build the TPM in a separate chip outside the main CPU too.

1. Has built-in private key with corresponding public key. The private key is secured at the hardware level and can never be taken out of the chip or read outside the chip. Its corresponding public key is however freely distributed similar to validating a https website's certificate's public key for authentication while connecting to that website. The TPM chip also can store other secrets with OS level security guarantees for access.
2. For TPM-based enrollment, the public key in a new IoT gateway residing in its CPU's TPM is registered. Its public key challenges the gateway, and when the gateway responds by encrypting the challenge text with its private key, and validates the public key, it is trusted.
So when hundreds of assets are deployed, manufacturers insert the software directly into those gateways and ship them directly from the factory to the customers' deployments. This way the effort and worry of bringing them to the deployment location to install such software, giving it credentials etc., can be distributed and anybody can go and plug it in to the network, turn on, connect to the INFER™ Server, authenticate itself and, get enrolled.
5. **Certificate-based Enrollment:** Unlike the TPM hardware's built-in certificate, a normal certificate file is assigned to the gateway by putting the certificate's private key inside the asset and use it to authenticate the asset's identity.

Note:

- TPM-based enrollment is hardware-based and built into the asset.
 - Certificate-based enrollment is a file distributed into the assets and used for authentication.
 - **3, 4, and 5** are used for individual and automated bulk register with CPU ID and pre-register all. As the assets arrive at their final location, wired up and turned on, on first boot, the script runs and invokes the enrollment CLI with right value of the CPU ID, and the Server knows that it was expecting the asset and begins to enroll them, and starts giving details from the Server.
6. **Security Whitelisting:** Considering the possibility of spoofing the CPU ID, serial number, or any other value deemed secure, to pre-empt such hacking efforts, an extra layer of Whitelisting is implemented.
 - Here, even when the asset's serial number is considered as the unique property for its authentication, this property can be kept disabled by default. Just before the administrator powers the asset on for the 1st time along with

network connection, he can log in via his mobile application and whitelist this asset. So, besides matching the asset's serial number, the Whitelisting process in asset enrollment gives the extra protection layer to the asset.

- Generally, hardware-based security is considered more reliable although the workflow is more complicated. In Property-based authentication, the MAC address can be spoofed. However any machine readable information inherent of the system, including serial number, or CPU ID read by the OS can be used as unique identifiers parsed as the value for the property and onboarded.
7. **Zero Touch Enrollment:** Register gateways in bulk using zero touch enrollment credentials. You must upload a `CSV` file with the hardware ID and model number of each gateway.

5.2 Onboarding a Gateway using Basic Authentication

Prerequisites: Before you onboard a gateway using the basic authentication method, you need to meet all the criteria listed below:

1. Ensure that you have the user name and password of the user in the organization where you want to enroll the asset. (`username` and `password`)
2. If you have accounts in multiple organizations, then ensure that you have the **Domain Name** for the Organization where the asset is to be enrolled. (`user-orgdomain-name`)
3. You must have created an asset template with **Basic Enrollment** as the **Provider Type**, and it must be available on INFER™ UI. (`template`)
4. By default, the asset will be enrolled in the Organization where the user's account exists. However, if you wish to enroll the asset in a sub-organization, then ensure that you have the **Organization ID** of the sub-org. (`device-org-id`)
5. You must have installed the Agent on your gateway.
6. You must know the name that you want to assign to your gateway in the INFER™ UI. (`name`)

To onboard a gateway using the basic authentication method, perform the following steps:

1. On the INFER™ UI, navigate the **Templates > Assets**.
2. Identify the asset template to be associated with your gateway.
3. Log in to your gateway and change the directory to:
 - **For Linux/MacOS:** `/opt/smarthub/iotc-agent/bin`
 - **For Windows:** `C:/Program Files/SmartHub/iotc-agent/bin`

Next, run the following command:

```
./DefaultClient enroll --auth-type=BASIC [--device
--orgid=<org domain id>]
--template=<template name> --name=<gateway name>
[--user-org-domain-name=<organization domainname>]
--username=<user name> [ --password=<prompt|file:<path>> ]
```

Note:

- If you are providing a file as input for the password, ensure that the file is accessible by the DefaultClient.
- For a successful enrollment, the response must be `0`.

4. You have successfully enrolled a gateway using the basic authentication method and have assigned a asset ID to it.
5. To verify that the gateway is enrolled, go to the INFER™ UI and click the **Monitored Assets** tab. You can see that the gateway is listed in the **Inventory - Monitored Assets** page and its status must be **ENROLLED**.

5.3 Onboarding a Gateway using Token-Based Authentication

Prerequisites: Before you onboard a gateway using the token-based authentication method, you need to meet all the criteria listed below:

1. You must have the **CREATE DEVICE** permission to perform this operation.
2. You must have created a asset template with **Token-based** as the **Provider Type**, and it must be available on the INFER™ UI.
3. You must have installed the Agent on your gateway.
4. You must know the name you are going to assign to your gateway in the INFER™ UI.

To onboard a gateway using the token-based authentication method, perform the following steps:

1. From the INFER™ UI, go the **Inventory > Monitored Assets > REGISTER > Gateway**. The **Register Gateway** pop-up appears.
2. Under **Asset Template**, from the drop-down menu, select your desired template that has Token-based Authentication enabled to associate with your gateway.
3. Under **Asset Name**, enter your desired gateway name.
4. Click **REGISTER**. You have successfully registered your gateway.
5. Now, your newly registered gateway appears listed in the **Asset - All Assets** page.
6. Next, create a credential to enroll your gateway. To do so, from the **Inventory - Monitored Assets** page, click the gateway that you just registered.
7. Click the **Actions** drop-down menu and select **Create Gateway Credentials**.
8. Click **CREATE**. The following pop-up appears as shown below:

Credential for Axis101

Provider Type Token Based

Expires on 07/24/2023, 8:53 PM (40 Days)

Credential

.....

This is a one-time credential that will be used for gateway enrollment

COPY

CLOSE

9. Click **COPY** to copy the token to the clipboard. The token expiry time that you set when creating the template appears.
10. Log in to your gateway and change the directory to:
 - ****For Linux/MacOS****: ``/opt/smarthub/iotc-agent/bin``
 - ****For Windows**** : ``C:/Program Files/SmartHub/iotc-agent/bin``
11. Run the following command:

```
./DefaultClient enroll --auth-type=TOKEN --  
token=<authenticationtoken>
```

Note: For a successful enrollment, the response must be `0`.

5.4 Onboarding a Gateway using Property-based Authentication

Prerequisites: Before you onboard a gateway using the property-based authentication method, you need to meet all the criteria listed below:

1. You must have the `CREATE_DEVICE` permission to perform this operation.
2. You must have installed the Agent on your gateway.
3. You must have created an asset template with **Property-based** set as **Provider Type**, and it must be available on the INFER™ UI.
4. You must know the name that you want to assign to your gateway in the INFER™ UI.

To onboard a gateway using the property-based authentication method, perform the following steps:

1. From the INFER™ UI, go to **Inventory > Monitored Assets > REGISTER > Single Gateway**. The **Register Gateway** pop-up is appears.
2. Under **Asset Template**, from the drop-down menu, select your desired template that has Property-Based Authentication enabled to associate with your gateway.
3. Under **Asset Name**, enter your desired gateway name.
4. Click **REGISTER**. You have successfully registered your gateway.
5. The newly registered gateway will appear listed in the **Inventory - Monitored Assets** page.
6. Next, you need to create a credential to enroll your gateway. To do so, from the **Inventory - Monitored Assets** page, click the gateway that you just registered.
7. Click the **Actions** drop-down menu and select **Create Gateway Credentials**. Click **CREATE**. The **Credentials** pop-up appears as shown below:

Credential for MAXIS CORE01

Provider Type Property Based

Identity Key JIUEKKFIHEUGU9894KKLNJB438HFJBSNKFMLKOI30IO

Value

JIUEKKFIHEUGU9894KKLNJB438HFJBSNKFMLKOI30IO

Credential

.....

This is a one-time credential that will be used for gateway enrollment

COPY

Copied To Clipboard

CLOSE

8. Enter a value for the keys that you defined when you created the asset template. The key and value pair must be unique for all the assets that you have configured under your Organization. The asset must send the same key and value pair to the Server.
9. Log in to your gateway and change the directory to
 - **For Linux/MacOS:** `/opt/smarthub/iotc-agent/bin`
 - **For Windows:** `C:/Program Files/SmartHub/iotc-agent/bin`
10. Run the following command:

```
./DefaultClient enroll --auth-type=PROPERTY --
key=<identitykey> --value=<correspondingvalue>
```

Note: For a successful enrollment, the response must be `0`.

5.5 Onboarding a Gateway using TPM-based Authentication

Note: TPM based enrollment is not supported for MacOS.

Prerequisites: Before you onboard a gateway using the Trusted Platform Module-based authentication method, you need to meet all the criteria listed below:

1. You must enable TPM from your gateway's BIOS settings.
2. You must have installed the Agent on your gateway.
3. To verify that TPM permissions and settings are in place, run the following command on your gateway:

```
[root@localhost ~]# su iotc -c /opt/
smarthub/iotcagent/bin/tpm_verify
```

The output must display the following response:

```
SmartHub secured.
```

- The following steps are mandatory for gateways running on Ubuntu operating systems:

- If `SmartHub secured` is not appearing, run the following commands on the gateway and rerun the `tpm_verify` command:

```
sudo groupadd --system tss
#This command creates a system level 'tss' group.

sudo useradd --system tss -g tss
#This command creates a system level 'tss' user and adds it to the 'tss'
  ↳ group.

sudo usermod -a -G tss iotc
#This command adds 'iotc' user to the 'tss' group.

sudo usermod -g tss iotc
#This commands makes 'tss' as the primary group of 'iotc'
```

- To run every time your gateway starts, add the following commands in a run script:

```
sudo chown tss:tss /dev/tpmrm0
#Changes the ownership of /dev/tpmrm0 from 'root:root' to 'tss:tss'.

sudo chmod g+rw /dev/tpmrm0
#Adds read+write permissions for group on the asset /dev/tpmrm0.
```

- You must have the `CREATE_DEVICE` permission to perform this operation.
- You must have created a asset template with **TPM Based** as the **Provider Type**, and it must be available on the INFER™ UI.
- You must know the name that you want to assign to your gateway in the INFER™ UI.

To onboard a gateway using the TPM-based authentication method, perform the following steps:

- From the INFER™ UI, go to **Inventory > Monitored Assets > REGISTER > Gateway**. The **Register Gateway** pop-up is appears.
- Under **Asset Template**, from the drop-down menu, select your desired template that has TPM-based Authentication enabled to associate with your gateway.
- Under **Asset Name**, enter your desired gateway name.
- Click **REGISTER**. You have successfully registered your gateway.
- Now, your newly registered gateway appears listed in the **Inventory - Monitored Assets** page.
- Next, you need to create a credential to enroll your gateway. To do so, from the **Inventory - Monitored Assets** page, click the gateway that you just registered.
- To enroll, log in to your TPM enabled gateway and run the following command:

- For Linux:** `/opt/smarthub/iotc-agent/bin/DefaultClient enroll --auth-type=TPM`

- **For Windows:**

```
C:/Program Files/SmartHub/iotc-agent/bin/DefaultClient enroll
↵ \--auth-type=TPM
```

8. To enable your TPM enabled gateway for an automatic enrollment, perform the following steps:

1. Go to:

- **For Linux:** /opt/smarthub/iotc-agent/bin/conf/iotc-agent.cfg

- **For Windows:**

```
C:/Program Files/SmartHub/iotc-agent/bin/conf/iotc-agent.cfg
```

The `iotc-agent.cfg` file lists the details about your gateway enrollment.

2. Scroll down to the `autoEnrollmentType` parameter and change its value to 1. This change enables your registered gateway to be enrolled automatically.

3. You can also configure the retry interval by specifying a `autoEnrollRetryIntervalSeconds` value. The INFER™ Server tries to enroll your whitelisted gateway after the specified interval. The default interval value is 300 seconds.

4. Save the configuration and restart the INFER Agent. The following example is a sample `iotc-agent.cfg` file for auto enrollment:

```
/opt/smarthub/iotc-agent/conf/iotc-agent.cfg
Auto Enrollment:
# Auto enrollment of a registered gateway. 0 - No auto
enrollment and 1 - TPM based
autoEnrollmentType = 1
# Enrollment retry interval in seconds, should be > 0
autoEnrollRetryIntervalSeconds = 300
```

You have successfully enrolled a TPM enabled gateway.

5.6 Onboarding a Gateway using Zero Touch Enrollment

Note: Zero Touch enrollment is not supported for MacOS

Prerequisites: Before you onboard a gateway using the Zero Touch Enrollment method, you need to meet all the criteria listed below:

1. You must have the `CREATE_DEVICE` and **ZERO TOUCH ENROLLMENT** permissions to perform this operation.
2. You must have created an asset template with **Zero Touch Enrollment** as the **Provider Type**, and it must be available on the INFER™ UI.
3. The gateway must be a **Dell** gateway running Ubuntu Server and must be Zero Touch Enrollment enabled.
4. You must have created a `CSV` file that contains the list of assets to enroll, along with the following columns:
 1. Hardware Id (mandatory)
 2. Model Number (optional)
 3. Property Value (optional)

To onboard a gateway using the Zero Touch Enrollment method, perform the following steps:

1. From the INFER™ UI, go to **Inventory > Monitored Assets > REGISTER > Single Gateway**. The **Register Gateway** pop-up is appears.
2. Under **Asset Template**, from the drop-down menu, select your desired template that has Zero Touch Enrollment enabled to associate with your gateway.

Note: The Zero Touch Enrollment **Enrollment Type** cannot be changed.

3. Under **Asset Name**, enter your desired gateway name.
4. Click **REGISTER**. You have successfully registered your gateway.
5. Click **Upload** to upload the **CSV** file that contains a list of Hardware IDs of your gateways.
 1. The first row is reserved for the property name.
 2. The **HardwareId** field is mandatory.
 3. The **Model Number** and **Property value** fields are optional.
 4. Any values and names provided after the first column appear as custom properties on the registered gateways.

1	HardwareId	ModelNo	Property1
2	Z001422012345	dell3k	propertyvalue1
3	Z002422012346	dell5k	propertyvalue2

6. Click **REGISTER**.

5.7 Re-enrollment of a Gateway

The gateway re-enrollment feature in INFER™ is designed to handle scenarios where the existing gateway becomes non-functional—such as due to a system crash, OS reimaging, hardware failure, or data corruption.

Re-enrollment is necessary when migrating to a new server environment where the previous gateway setup is no longer valid. Before initiating re-enrollment, it is essential that the agent is installed and properly configured on the new server to ensure a secure and seamless transition.

Note:

If the agent is no longer running on the original device, but data files and enrollment details are still present then you must first uninstall the agent from the old device. Then, install a fresh agent on the new device.

This process helps maintain uninterrupted connectivity and ensures compliance with INFER's security protocols.

Re-enrollment works with both property-based and token-based enrollment. Verify that the agent is installed and running.

1. On the INFER™ UI, select the gateway you want to re-enroll and change it into maintenance mode.
2. Navigate to **Actions > Create Gateway Credentials**.
3. For token-based enrollment, copy the generated authentication token.

For Linux and Mac:

1. Open Terminal.
2. Navigate to:

```
/opt/smarthub/iotc-agent/bin/
```

Run the command:

```
./DefaultClient enroll --auth-type=TOKEN --token=<authentication token>
```

3. Once the re-enrollment is complete, run a sync command to bring up all connected devices:

```
./DefaultClient sync
```

For Windows:

1. Open PowerShell.
2. Navigate to:

```
"C:\Program Files\Smarthub\iotc-agent\bin\"
```

Run the command:

```
./DefaultClient enroll --auth-type=TOKEN --token=<authentication token>
```

3. Once the re-enrollment is complete, run a sync command to bring up all connected devices:

```
./DefaultClient sync
```

4. For a property based enrollment:

Run the command:

```
./DefaultClient enroll --auth-type=PROPERTY --  
key=<identity_key> --value=<corresponding_value>
```

5. Once the re-enrollment is complete, run a sync command to bring up all connected devices:

```
./DefaultClient sync
```

This may take some time depending on the number of devices connected to the gateway. Restart the agent to ensure all configurations are correctly applied by running the command.

```
systemctl restart iotc-agent.service
```

5.8 Whitelisting an Asset

A whitelist is an explicit listing of gateways that are allowed for enrollment.

The whitelisting option allows you to control the gateways that are allowed to enroll and the gateways that are not permitted to enroll. A whitelisted gateway is a virtual gateway created on the INFER™ Server.

The virtual gateway is registered but not enrolled, and it does not have a physical gateway associated to it until a physical gateway is enrolled using the TPM-based authentication method. After registering a gateway using a asset template that has the **Requires Whitelisting** option enabled, select **Whitelist** from the **Actions** drop-down menu to enroll the gateway.

5.9 Using Package Management CLI to Register Multiple Assets

You can use the Package Management CLI tool to register multiple assets to INFER™ using the Basic, Property-based, TPM-based, and Token-based enrollment types.

Ensure that you create a *JSON* file with the asset template name, list of assets, their credentials, and properties, in the following format:

```
{
  "templateName": "property-template",
  "devices": [{
    "name": "Agent_x86_2",
    "credential": [{
      "key": "Serial Number",
      "value": "abc-56 4d fa a4 78 fa f2 88-24 3a 14 11 7d bd b8 b6"
    }],
    "property": [{
      "name": "model",
      "value": "xx 5K"
    }, {
      "name": "color",
      "value": "white"
    }]
  }, {
    "name": "Agent_x86_3",
    "credential": [{
      "key": "Serial Number",
      "value": "abc-56 4d 13 fb cc 73 82 2e-08 5d b1 c1 38 bf 1d 23"
    }],
    "property": [{
      "name": "model",
      "value": "xyi3b"
    }]
  }
]
}
```

The **Package Management CLI** tool uses this JSON file to read the assets list and register them to INFER™.

1. Download the Package Management CLI tool to your system. The Package Management CLI tool contains the following set of asset commands that enable you register your assets in bulk:

```
a01:iot-cli xyz$ ./bin/darwin_amd64/package-cli devices
```

Manage assets on INFER IoT Center

Usage:

```
package-cli devices [command]
```

Available Commands:

register Register device by given name on INFER IoT Center

register-all Register multiple devices to INFER IoT Center.

Expects JSON file with device details.

search Search given device by name on INFER IoT Center

Flags:

-v, --api-version string INFER API version to use (default "1.0")

-h, --help help for devices

-s, --host-name string INFER IoT Center instance hostname <Required>

-i, --insecure Skip SSL certificate verification

-l, --log-file-path string Log file path (default "./iotcli.log")

Use "package-cli devices [command] --help" for more information about a
↪ command.

2. Run the register-all command with the path to the JSON file that you created.

```
a01:iot-cli xyz$ ./package-cli devices register-all
./example-iotc-package/device-regd-property-based.json -s
https://10.92.85.41 -i
Username: sysadmin
Password:
Authentication successful.
Registering device...
Device registered with id: 30d75156-65b7-4658-b1e1-e7fba5008122 name:
  ↪ Agent_x86_2
Updating device property...
Property update successful for device
Creating device credentials...
Device credential successfully created for device
Registering device...
Device registered with id: a8f2dddb-8631-4d02-bfcdb77febbf3a56 name:
  ↪ Agent_x86_3
Updating device property...
Property update successful for device
Creating device credentials...
Device credential successfully created for device

Successfully registered devices: 2
Total devices: 2
```

3. The registered assets are listed in the **Inventory - Monitored Assets** page of the INFER™ UI.

5.10 Registering Multiple Gateways

To register Gateways in bulk, perform the following steps:

1. From the INFER™ UI, go to **Inventory > Monitored Assets > REGISTER > Multiple Gateways**. The **Register Gateway** pop-up is appears. The **Bulk Register Gateways** wizard appears as shown below:

Bulk Register Gateways

1 Asset Template

3 Upload Gateway Details

4 Register Gateways

5 Summary

Select Asset Template

Select the Asset Template for which you wish to Register Gateways

Asset Template

Select Asset Template

CANCEL NEXT

- Under **Asset Template**, use drop-down menu to select the asset template to be used to bulk register gateways. The **Custom Properties** defined in the selected asset template appears.

Note: Only one asset template can be used to register multiple gateways at a time.

- Click **NEXT**.

- As per the asset template chosen by you in step 2., **Token Based Enrollment** or **Property Based Enrollment** will appear next.

- For **Token Based Enrollment**, toggle the **Generate Tokens** switch to generate tokens as asset identities to all the gateways being enrolled. For more information, see [Onboarding a Gateway Using Token-Based Authentication](#).
- For **Property Based Enrollment**, toggle the **Setup Gateway Credentials** switch to toggle option.

Note: After Registration, an enrollment Token will be generated for each Gateway.

- Click **NEXT**.

- Under **Upload Gateway Details**, download the **CSV** template file.

- Open the downloaded **CSV** template file in an appropriate application such as **Microsoft Excel**. As shown below, you will see the **Asset Name** as the first column followed by columns with names matching the custom properties defined in the gateway template you selected previously. The **Asset Name** is a mandatory field.

	A	B	C	D	E	F	G
1	Device-Name	Adapter-Camera-IP	Location-Country	Location-State	Location-City	Location-Floor	Device-Date-Deployment
2	TP-Link Tapo C200	183.37.194.135	India	Karnataka	Bengaluru	GF	01/01/2021
3	Qubo Smart Cam 360	192.168.0.90	United State	Utah	Salt Lake City	Third	
4	TP-Link Tapo C100	192.168.100.1	United State	Arizona	Phoenix		21/08/2021
5	Srihome SH025 camera	192.168.1.108	India		Delhi	FF	

- For each of the gateway assets that you want to bulk register, enter its **Asset-Name** and the required custom properties into the **CSV** file, one-per-row.

Note:

- After Registration, an enrollment Token will be generated for each Gateway.
- You can find the list of Custom properties essential for enrolling the asset, in the Adapter documentation or the Thing template's description. For assets connected via a TCP/IP network, these would be **IP Address**, and login credentials.

- Ensure to save the file to disk in its original **CSV** format.

- Drag and drop the filled **CSV** file in to the marked area or click the area as shown below:

Upload File (CSV)

Drag and drop Or click here to upload the CSV File

- Click **NEXT**.

- Under **Register Gateways**, review the details.

- Click **Start Registration**.

- Click **NEXT**.

- Click **DOWNLOAD** to download the **CSV** file.

Note: The Enrollment Tokens for the registered gateways can be found in the 2nd column of the **CSV** file.

16. Click **DONE**.

6 Working with INFER™ Agent

This chapter provides information about working with the INFER™ Agent.

The Agent is a daemon that resides on the Gateway. It acts as a conduit to the Server abstracting functionalities like enrollment, sending telemetry, processing commands, and OTA jobs scheduled by the IOTC service. In addition, it also offers an SDK each for Python and C that exposes APIs. Third-party applications can use these APIs on the Gateway to interact with.

The INFER™ Agent makes an outbound connection to the Server on port 443 (HTTPS).

From within a Gateway, the INFER™ Agent's software developer kit (SDK) called as **IoTCAgent** provides **C** APIs to interact with INFER™.

The IoTCAgent SDK contains the following:

- Two libraries:
 1. **iotc-agent-sdk**
 2. **iotc-agent-common**
- A header file: `iotcAgent.h`
- A sample: `DefaultClient.c`

6.1 Installing INFER™ Agent

This section lists the steps to install the INFER™ Agent on gateways that run on Windows and Linux operating systems.

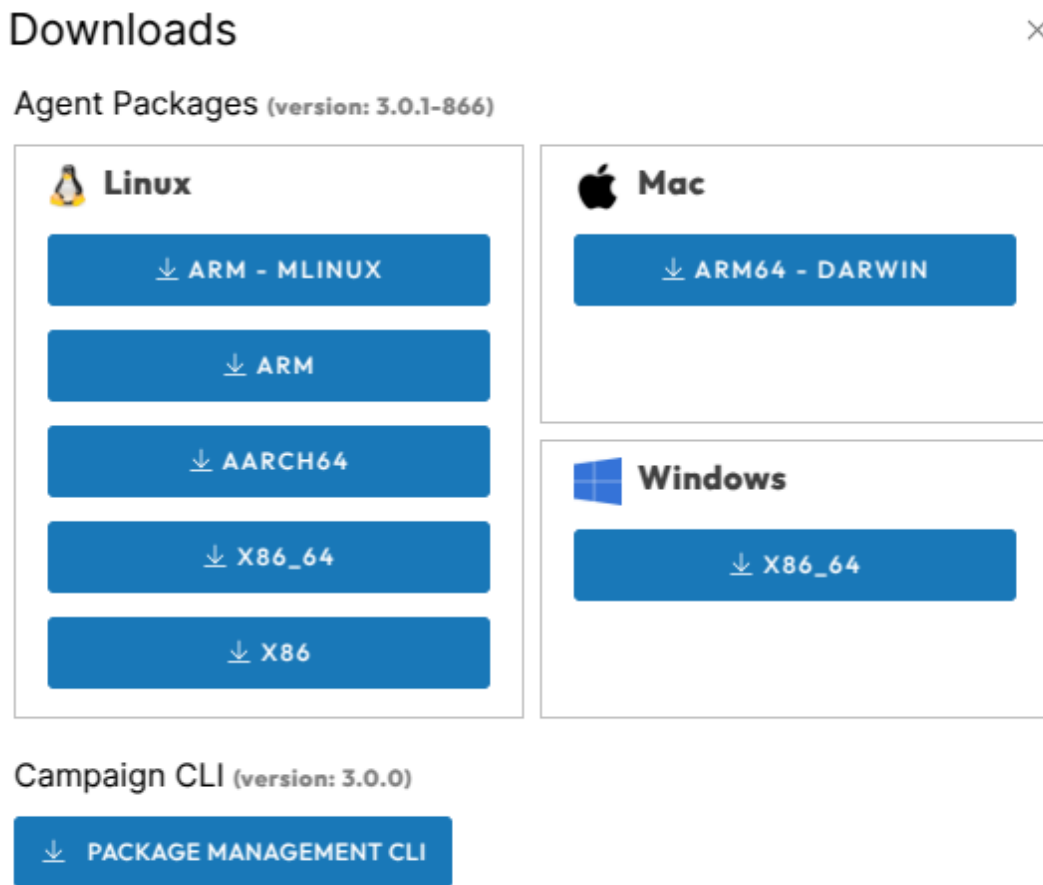
Prerequisites

- Verify that you have access to Linux Gateway with sudo privileges.
- Verify that INFER™ UI is reachable from the Linux Gateway. You can use *curl* or *wget* to try to access the SmartHub INFER™ UI to see if the portal is accessible.
- Verify the availability of python3 on the Linux Gateway. This can be verified by running `python3 --version`.
- Verify the availability of python3-pip on the Linux Gateway. This can be verified by running `pip3 --version`.
- Linux Gateway supports a multitude processor architectures for Linux and this includes x86_64, x86, arm, arch64 processor architectures. Make sure to download the agent for the right processor architecture for a successful agent installation. If in doubt run `uname -m` to know the machine architecture on the target gateway.
- In case the network demands that the all web interactions happens through a forwarding proxy, INFER™ Agent supports HTTP Proxy with or without authentication. Support is limited to HTTP Proxy only at this point in time. The proxy details including the proxy server url and any authentication credentials will be required for a successful onboarding of the INFER™ Agent. The need for a proxy configuration arises when the service is on the Cloud and in this particular case INFER™. If the proxy intercepts HTTPS connections as a Man-in-the-Middle (MITM), then the root Certificate Authority (CA) certificate from the proxy server is required. Please consult your IT administrator to obtain this certificate before starting the onboarding process.

6.1.1 Installing INFER™ Agent on Linux Gateway

Follow the steps listed below to download and install the INFER™ Agent on your Linux gateway.

1. On the INFER™ UI, click the **Download** icon on the top right. The following pop-up appears:



2. Download the **INFER™ Agent** tarball for the right processor architecture to your local system.
3. Using an FTP/SFTP application such as scp, WinSCP or FileZilla, you can transfer INFER™ Agent tarball to the gateway file system.
4. Alternately, you can also directly download the INFER™ Agent from the INFER™ Console to the target gateway. On the target gateway create a folder for INFER™ using the `mkdir INFER`.
5. On the command-line interface, use `curl` or `wget` commands to download target gateway. For example: if the infer server url is `iotc001-INFER.smarthub.ai`.

```
curl -Lo INFERagent.tar.gz
  ↪ "https://iotc001-INFER.smarthub.ai/api/iotc-agent/iotc-agent-$(uname
  ↪ -m)-3.0.1-latest.tar.gz"
```

OR

```
wget -O INFERagent.tar.gz
  ↪ https://iotc001-INFER.smarthub.ai/api/iotc-agent/iotc-agent-$(uname
  ↪ -m)-3.0.1-latest.tar.gz
```

In the above example, substitute the sever url with your INFER url.

6. The download process in step 5 can fail if the network on which the gateway resides

relies on a forwarding proxy. Both `curl` and `wget` supports supplying a HTTP proxy configuration as a part of the command line invocation or by setting an environment variable. Please note that INFER™ Agent only supports a HTTP forwarding proxy as of now.

When using an environment variable, use the following format to configure your http proxy in your current terminal.

For non-authenticating proxies

```
export http_proxy="http://proxy.example.com:8080"
export https_proxy="http://proxy.example.com:8080"
```

For authenticating proxies

```
export http_proxy="http://user:password@proxy.example.com:8080"
export https_proxy="http://user:password@proxy.example.com:8080"
```

The above are examples and one must substitute the values relevant to your network.

Download the INFER™ Agent with the following command:

```
curl -kLo INFERagent.tar.gz
↪ "https://iotc001-INFER.smarthub.ai/api/iotc-agent/iotc-agent-$(uname
↪ -m)-3.0.1-latest.tar.gz"
```

OR

```
wget --no-check-certificate -O INFERagent.tar.gz
↪ "https://iotc001-INFER.smarthub.ai/api/iotc-agent/iotc-agent-$(uname
↪ -m)-3.0.1-latest.tar.gz"
```

7. Extract the INFER™ Agent tarball on the gateway. For example, `tar -xvzf INFERagent.tar.gz`
8. In proxied environments, for the INFER™ Agent to connect to INFER™ Console, the proxy information must be added to the INFER™ Agent configuration before the install. The agent configuration can be found at `iotc-agent/conf/iotc-agent.conf`.

Use any of your editor on the terminal to alter the following values:

```
# Supported proxy types - NO_PROXY, HTTP_PROXY
proxyType = HTTP_PROXY
proxyServerIP = proxy.example.com
proxyServerPort = 8080
proxyServerUsername = user
proxyServerPassword = password
```

Note that if the forward proxy is non authenticating, leave the `proxyServerUsername` and `proxyServerPassword`

The above proxy configuration must also be entered in the Gateway Template settings before the enrollment process. To know more about asset templates, refer to Section **Agent Settings**, in [Working with an Asset as a Template](#).

If the forwarding proxy acts as a Man-In-Middle (MiM), for https connections, it will be required to append Root CA presented by the proxy server to the Infer Agent Trust store which can be found at `iotc-agent/ca.crt`. We recommend talking to your proxy administrator to get this certificate. However, if the proxy server is configured to return its

certificate chain, you could also get the same in certain cases using the following command:

```
echo q | openssl s_client -connect proxy.example.com:port -showcerts
```

The last certificate in the returned chain including and beginning with:

---BEGIN CERTIFICATE---

```
MIIFBTCCAu2gAwIBAgIQS6hSk/eaL6JzBkuoBI110DANBgkqhkiG9w0BAQsFADBP    KP-  
pdzvvtTnOPIC7SQZSYmdunr3Bf9b77AiC/ZidstK36dRILKz7OA54=
```

---END CERTIFICATE---

is what you must copy and append.

9. Change the directory to `iotc-agent` and run `install.sh` as `sudo` .

```
`sudo ./install.sh`
```

10. Verify whether the Daemon and the Agent services are running. View the **syslog** or use the `systemctl status iotc-agent.service` command.

Note: GRPC errors are common and expected at this stage.

6.1.2 Installing INFER™ Agent on a MacOS Gateway

INFER™ Agent supports any MacOS device with M1 chipset or higher. The versions of Mac running on Intel hardware are NOT supported as of now.

Prerequisites:

- Have access to MacOS Gateway with sudo privileges.
- INFER™ UI is reachable from the MacOS Gateway. You can launch a browser and try to access the SmartHub INFER™ UI to see if the portal is accessible.
- Verify the availability of python3 on the MacOS. This can be verified by running `python3 --version`
- Verify the availability of python3-pip on the MacOS. This can be verified by running `pip3 --version`

Follow the steps listed below to download and install the INFER™ Agent on your MacOS gateway.

1. On the INFER™ UI, click the **Download** icon on the top right. The following pop-up appears:

Downloads



Agent Packages (version: 3.0.1-866)

Linux

↓ ARM - MINUX

↓ ARM

↓ AARCH64

↓ X86_64

↓ X86

Mac

↓ ARM64 - DARWIN

Windows

↓ X86_64

Campaign CLI (version: 3.0.0)

↓ PACKAGE MANAGEMENT CLI

- Click the MacOS download button. The INFER™ Agent zip file **INFER™ Agent (ARM64)** gets downloaded to your local machine. The agent file format is `iotc-agent-darwin-arm64-<<version>>-latest.tar.gz`.

For example, `iotc-agent-darwin-arm64-3.0.1-latest.tar.gz`

- Once the agent is downloaded to the *Downloads* directory on your home folder, extract the Agent tarball. Launch the terminal:

```
cd ~/Downloads
tar -xvf iotc-agent-darwin-arm64-3.0.1-latest.tar.gz
```

- In proxied environments, for the INFER™ Agent to connect to INFER™ Console, the proxy information must be added to the INFER™ Agent configuration before the install. The agent configuration can be found at `iotc-agent/conf/iotc-agent.conf`.

Use any of your editor on the terminal to alter the following values

```
# Supported proxy types - NO_PROXY, HTTP_PROXY
proxyType = HTTP_PROXY
proxyServerIP = proxy.example.com
proxyServerPort = 8080
proxyServerUsername = user
proxyServerPassword = password
```

Note that if the forward proxy is non authenticating leave the `proxyServerUsername` and `proxyServerPassword`

The above proxy configuration must also be entered in the Gateway Template settings

before the enrollment process. To know more about asset templates, refer to Section **Agent Settings**, in [Working with an Asset as a Template](#).

If the forwarding proxy acts as a Man-In-Middle (MiM), for https connections, it will be required to append Root CA presented by the proxy server to the Infer Agent Trust store which can be found at `iotc-agent\ca.crt`. We recommend talking to your proxy administrator to get this certificate. However, if the proxy server is configured to return its certificate chain, you can also get the same in certain cases using the following command:

```
echo q | openssl s_client -connect proxy.example.com:port -showcerts
```

The last certificate in the returned chain including and beginning with

```
---BEGIN CERTIFICATE---
```

```
MIIFBTCCAu2gAwIBAgIQS6hSk/eaL6JzBkuoBI110DANBgkqhkiG9w0BAQsFADBP    KP-  
pdzvvtTnOPIC7SQZSYmdunr3Bf9b77AiC/ZidstK36dRILKz7OA54=
```

```
---END CERTIFICATE---
```

is what you must copy and append.

5. Now run `install.sh` as `sudo`

```
sudo ./iotc-agent/install.sh
```

6. Verify whether the Daemon and the Agent services are running. To view if the agent service is installed and running, use the following commands one at a time from shell.

```
sudo /opt/smarthub/iotc-agent/bin/iotc-agent-cli ping
```

The expected output of the above command should be *CommandPing successful*.

7. Optionally, agent running logs can be viewed using the following command:

```
sudo log stream --predicate 'process == "iotc-agentd"' --info --color auto
```

8. Press Ctrl+C to exit the log stream.

Note: You can safely ignore the GPRC errors in the log messages.

You have successfully installed the INFER™ Agent.

The next important step post the installation of the INFER™ Agent is onboarding MacOS gateway into INFER™ UI. For more information, see [Onboarding Gateways](#).

6.1.3 Installing INFER™ Agent on Windows Gateway

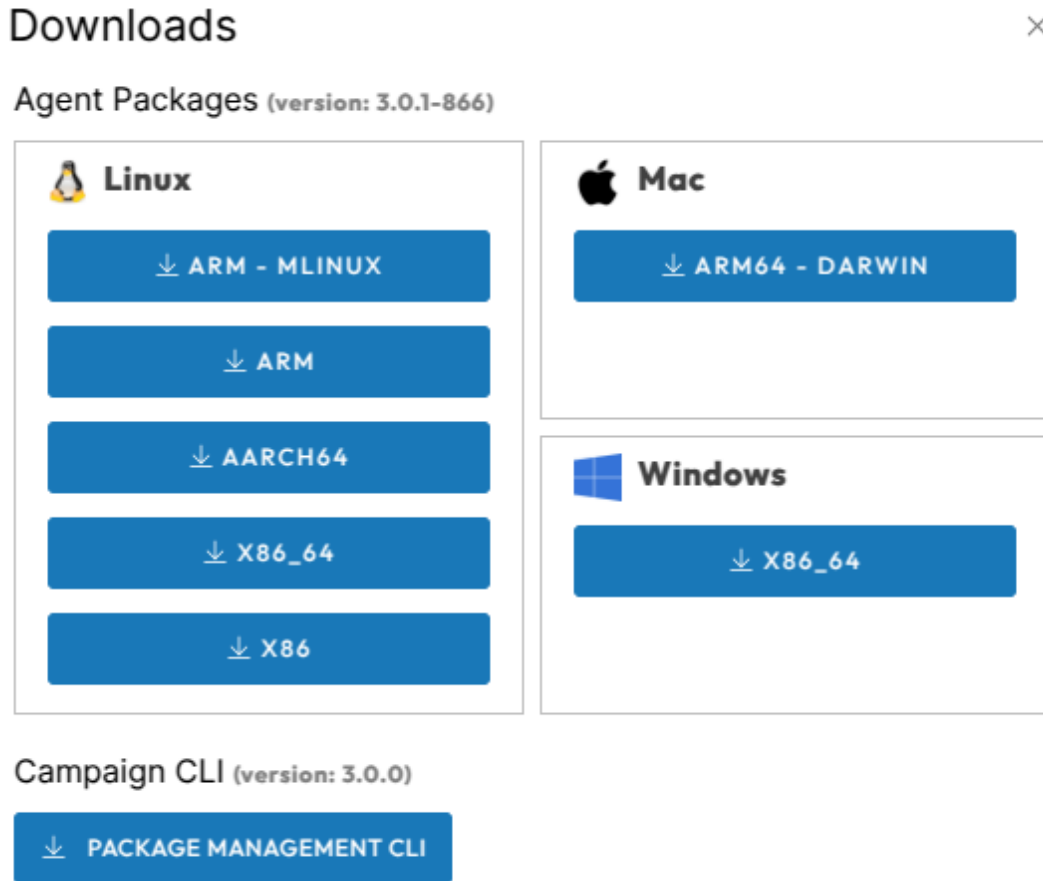
Perform the steps listed below to download and install the INFER™ Agent on your Windows gateway.

- Supported operating systems:
 - Windows 10 IoT Enterprise (x64)
 - Windows 10 IoT Core (x64, ARM)
 - Windows Embedded Standard 7 (x64)
 - Windows 7 X64 with SP 1

Note: Windows Embedded Standard 7 (x64) requires Windows PowerShell v2.0 or later to be installed on your system.

- Available INFER™ Agent binaries:

- Windows 10 x64 (any edition):
`'iotc-agent-windows-x86_64-<ve`
- 1. On the INFER™ UI, click the **Download** icon on the top right. The following pop-up appears:



2. Download the INFER™ Agent tarball **INFER™ Agent (x86_64)** to your local system.
3. Copy the zip file to the gateway file system.
4. Extract the zip file on the gateway by running the following PowerShell command.

Command prompt:

```
> powershell.exe -command "Expand-Archive -Force <zipfile> <target-folder>"
```

5. Run the PowerShell script *install.ps1* with administrator privileges.

Command prompt:

```
> powershell.exe -ExecutionPolicy ByPass -File  
install.ps1
```

PowerShell prompt:

```
> Set-ExecutionPolicy ByPass  
> & install.ps1
```

6. In proxied environments, for the INFER™ Agent to connect to INFER™ Console, the proxy information must be added to the INFER™ configuration before the install. The agent configuration can be found at `iotc-agent\conf\iotc-agent.conf` for the

extracted Agent.

Use any editor on the terminal to alter the following values:

```
# Supported proxy types - NO_PROXY, HTTP_PROXY
proxyType = HTTP_PROXY
proxyServerIP = proxy.example.com
proxyServerPort = 8080
proxyServerUsername = user
proxyServerPassword = password
```

Note that if the forward proxy is non authenticating leave the `proxyServerUsername` and `proxyServerPassword`

The above proxy configuration must also be entered in the Gateway Template settings before the enrollment process. Please refer to Section **Agent Settings**, in [Working with an Asset as a Template](#).

If the forwarding proxy acts as Man-In-Middle(MIM), for https connections, it will be required to append Root CA presented by the proxy server to the INFER™ Agent Trust store which can be found at `iotc-agent\ca.crt`. We recommend talking to your proxy administrator to get this certificate.

7. Run the PowerShell script `install.ps1` with administrator privileges.

```
Command prompt:
> powershell.exe -ExecutionPolicy Bypass -File
install.ps1

PowerShell prompt:
> Set-ExecutionPolicy Bypass
> & install.ps1
```

8. The INFER™ Agent for Windows is installed at Bash `C:\\Program Files\\SmartHub\\iotc-agent`

6.2 Working with IoTCAgent CLI

The **IoTCAgent CLI** is IoTCAgent's default client binary `DefaultClient`. On Windows, this tool is available as `DefaultClient.exe`

This tool provides a command-line interface (CLI) to perform IoTCAgent SDK operations. Using the **IoTCAgent CLI** tool, you can build a client that operates with using the IoTCAgent SDK. You can use the `DefaultClient` binary as a reference for building your client.

The **IoTCAgent CLI** provides multiple CLI options. Please run the following command to know more.

```
/opt/smarthub/iotc-agent/bin# ./DefaultClient help
```

You can use the IoTCAgent CLI to rapidly perform operations such as enrolling a device and setting properties for a device.

Note: Declare the library path explicitly if you see error messages such as:

```
error while loading shared libraries: libiotc- agentsdk.so:
cannot open shared object file: No such file or directory
```

Run the following command:

```
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/smarthub/iotc-agent/lib/
```

The **IoTCAgent CLI** is available in the bin directory of IoTCAgent:

```
/opt/smarthub/iotc-agent/bin/DefaultClient
```

6.2.1 Using DefaultClient Daemon

You can run the `DefaultClient` binary file as a daemon process in the background. In the daemon mode, **DefaultClient** connects to the IoT Agent daemon and authorizes campaign call-backs automatically.

It also fetches commands from the Server at regular intervals. When additional options are specified, **DefaultClient** gathers the default CPU and Memory Usage metrics from the Gateway device and sends them periodically.

You can perform the following operations using the **DefaultClient** daemon:

- Start the **DefaultClient** daemon without sending the default metrics:

```
$ DefaultClient start-daemon
```

- Start the `DefaultClient` daemon with default metrics every 10 minutes:

```
$ DefaultClient start-daemon \--device-id=<device_id> \--interval=600
```

- Stop the `DefaultClient` daemon.

```
$ DefaultClient stop-daemon
```

Using the IoT Agent connection, the `DefaultClient` daemon accepts requests from the following pipe files if necessary:

- `/tmp/iotc-defclient/input` for an input request.
- `/tmp/iotc-defclient/output` for an output request.

The following sample illustrates how to get system properties using the `DefaultClient` daemon:

```
$ echo "get-properties --device-id=l3c425e1-873a-43f0-a529-cb05289a8a40 --type=system" > /tmp/iotc-defclient/input
$ cat /tmp/iotc-defclient/output
```

6.3 Updating INFER™ Agent

You can update the INFER™ Agent from the **Inventory > Monitored Assets** tab or by using OTA campaigns.

For information about compatible INFER™ Server and Agent versions, see the [INFER™ Release Notes](#).

6.3.1 Updating INFER™ Agent Using Campaigns

Update the Agent to a newer version using OTA Campaigns.

Prerequisite: You must be a **Campaign Administrator** to perform this operation.

When upgrading the Server, IoT Agent packages are created for each target OS and architecture, and are displayed in the **Packages** tab of the Console. These packages contain the specifications required to upgrade the Agent.

As a Campaign Administrator, you can create a campaign with this IoT Agent package and target it to run on those gateways that require an agent upgrade.

Note: Ensure that you select the correct version of the IoT Agent package when upgrading the Agent.

For more information about creating and running campaigns, see [Working with Campaigns](#).

6.3.2 Updating INFER™ Agent on Multiple Assets

Update the INFER™ Agent on multiple assets from the **Inventory > Monitored Assets** tab.

Prerequisite: You must be a **Device Administrator** to perform this operation.

Perform the following steps:

1. On the INFER™ UI, navigate to **Inventory > Monitored Assets**.
The **Inventory-Monitored Assets** page lists the registered, enrolled, and unenrolled Gateway and Thing assets.
2. Select the assets for which you want to update the agent.
Note: You can also select assets from different templates.
3. From the ... (ellipsis) drop-down menu, select **Update Agent**.
4. Click **Confirm**.

The **Update Agent Package** confirmation dialog box displays the current version and the upgrade version of the agent.

Note: You can verify the status of the INFER™ Agent update on multiple assets using the **Tasks** tab.

For more information, see [Tasks](#).

6.3.3 Updating INFER™ Agent on a Device from the Console

You can update the INFER™ Agent on a specific gateway device from the INFER™ Console.

Prerequisite: You must be a **Device Administrator** to perform this operation.

Perform the following steps:

1. On the INFER™ UI, navigate to **Inventory > Monitored Assets**.
The **Inventory - Monitored Assets** page lists the registered and enrolled gateway and Thing assets.
2. Click the device for which you want to update the agent.
3. From the **Actions** drop-down menu, select **Update Agent**.

The **Update Agent Package** confirmation pop-up displays the current version and the upgrade version of the agent.

4. Click **CONFIRM**.

The agent upgrade process is initiated. To view the status of the agent update, click the **Commands** tab. To download, click the download icon against the command.

6.3.4 Updating INFER™ Agent on a Device interactively via Shell

The instructions provided below are for a Linux gateway but will work the same way on a Windows gateway when they are run with the appropriate paths.

Prerequisite: You must login into the gateway from a shell prompt as a user with **root** or **sudo** privileges

1. Confirm that you have an agent running already. The following command will print the agent version:

```
cat /opt/smarthub/iotc-agent/version
```

2. Change directory to where you have the new agent and unpack the tarball.

```
cd /home/user/downloads/  
tar -xf iotc-agent.xyz.tar.gz  
cat ./iotc-agent/version
```

3. Now run the upgrade script.

```
/opt/smarthub/iotc-agent/script/upgrade.sh  
/home/user/downloads/iotc-agent/ 1234
```

Note: When you run the upgrade, make sure your current directory is neither the old agent nor the new agent.

6.4 Uninstalling INFER™ Agent

This section lists the steps to uninstall the INFER™ Agent on gateways that run on Windows and Linux operating systems.

6.4.1 Uninstalling INFER™ Agent on Linux Gateway

Follow the steps listed below to uninstall the INFER agent on gateways that run on Linux operating system.

1. ON the terminal, run the following command:

```
sudo /opt/smarthub/iotc-agent/uninstall.sh
```

2. The following message is displayed when you successfully uninstall:

Uninstallation of iotc-agent done successfully

6.4.2 Uninstalling INFER™ Agent on Windows Gateway

Follow the steps listed below to uninstall the INFER agent on gateways that run on Windows operating system.

1. Open PowerShell in Administrator mode.
2. Navigate to the directory:

```
cd "C:\Program Files\Smarthub\"
```

3. Run the uninstall command:

```
.\iotc-agent\uninstall.ps1
```

Or run:

```
`& "C:\Program Files\Smarthub\iotc-agent\uninstall.ps1"
```

2. The following message is displayed when you successfully uninstall:

Uninstallation of iotc-agent done successfully

6.4.3 Uninstalling INFER™ Agent on MacOS Gateway

1. On the terminal, run the following command:

```
sudo /opt/smarthub/iotc-agent/uninstall.sh
```

2. The following message is displayed when you successfully uninstall:

Uninstallation of iotc-agent done successfully

6.5 Firmware Updates for an Asset

Firmware updates for assets are available in the System properties of an asset.

1. On the INFER™ UI, perform an **Advanced Search**.
2. Select your Asset template, **Key** as **Asset-Model**, and **Firmware-version**.
3. Enter *parentgatewayid* in Columns. Save your query. **Note:** Change the operator to *Not equal to*. This is to avoid overwriting assets that already have the latest firmware.
4. Upload a **Package Builder** and enter the Firmware's latest Version.
5. Attach the *InstalldeviceFirmware.sh* and *installdeviceversion.bin* files.
6. Under **Manifest > Headless Execution** appears switched ON by default. This controls the automatic transition of each lifecycle phase without any interaction.
7. Under **Lifecycle** from the drop-down menu, select and add the package's desired lifecycle phase.
8. Provide a Valid Action and its associated Arguments. Click **Done** and Review the summary to run a Firmware Update.

7 Onboarding Connected Things

This chapter details the steps required to onboard Things individually or in bulk.

Once your Gateway is registered or onboarded and the required **Adapters** are deployed, you can onboard your **Things** by performing the steps below:

1. Create a **Thing Template** by following instructions in "Creating a Device Template".
2. Ensure that this Thing Template is added under **Connected Device Templates** to the corresponding **Gateway Template**.

The process to onboard Things depend on how your assets are deployed and the protocol used by the Adapters to talk to the Things. These two factors determine whether the Adapter can **discover** Things automatically or not.

Note: If the Adapter is capable of automatically discovering Things, it would **Register** and **Enroll** them into INFER™. In that case, you can skip the rest of this section.

If the Adapter cannot automatically discover connected Things, you need to **Register** them first via the INFER™ Console and set appropriate **Custom Properties** for the Things.

Here, the Adapter uses the information in the registered Things' Custom properties, to connect to the assets and enroll them into INFER™.

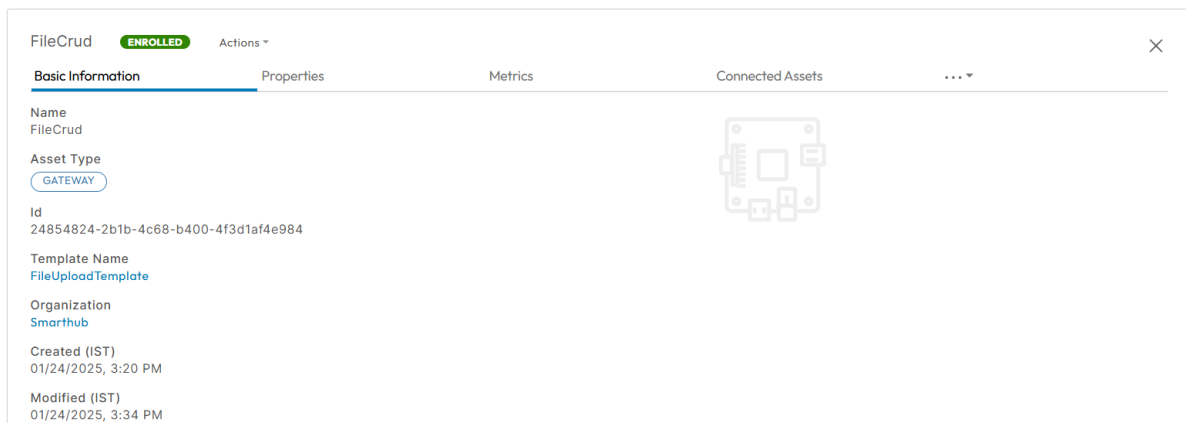
Note: You can register Things one by one, or in bulk.

7.1 Registering Things One by One

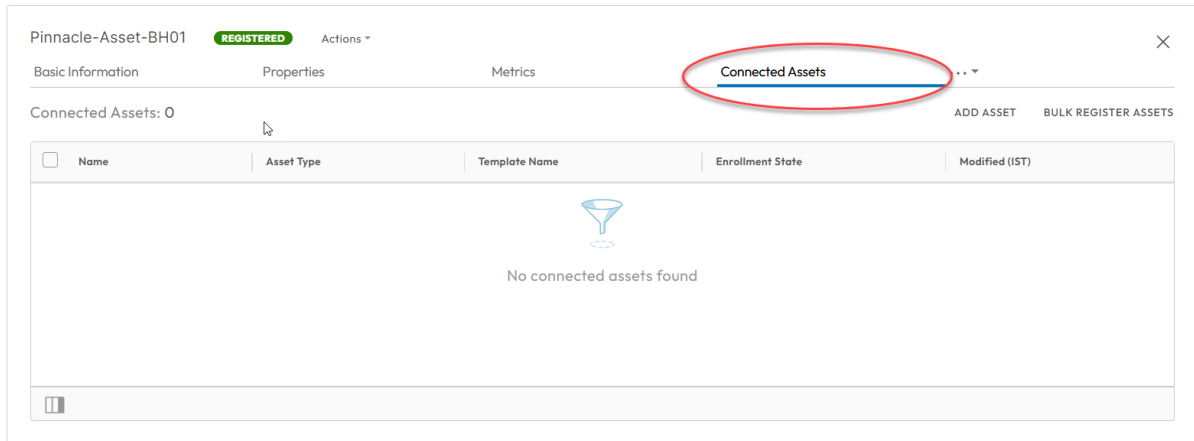
To register assets one by one, perform the following steps:

1. Under **Inventory - Monitored Assets**, click the desired Gateway. The Gateway information appears as follows:

Inventory - Monitored Assets



2. Click the **Connected Assets** tab as highlighted below:



- Under **Connected Assets**, click **ADD Asset**. The **Register Connected Device** pop-up appears as follows:

- Select the desired **Asset Template** from the drop-down menu and enter the **Asset Name** as highlighted above.
- Click **REGISTER**. The **Connected Assets** page appears as below displaying the newly registered device:

The screenshot shows the 'GATEWAY' interface with the 'ENROLLED' status and 'Actions' dropdown. The 'Connected Assets' tab is active, displaying a device topology and a table of assets.

Device Topology: A diagram showing a 'GATEWAY' node connected to a 'New registered Thing' node, which is further connected to an 'avigilon camera' node. A red box highlights the 'New registered Thing' node, and another red box highlights the 'avigilon camera' node. A red arrow points from the 'New registered Thing' node to the 'avigilon camera' node.

Assets Table:

<input type="checkbox"/>	Name	Asset Type	Template Name	Enrollment State	Modified (IST)
<input type="checkbox"/>	avigilon camera	Thing		Enrolled	01/22/2025, 4:08 PM

- To view this Thing's details, click the registered Thing in the Device topology above or in the table available below the topology.
- Next, go to the **Properties** tab and click Edit icon next to **Custom Properties** as highlighted below:

The screenshot shows the 'FileCrud' interface with the 'ENROLLED' status and 'Actions' dropdown. The 'Properties' tab is active, displaying a search bar and two columns of properties: 'System Properties' and 'Custom Properties'.

Search in Properties: Search: ☒ System ☒ Custom

System Properties:















- > iotc
- > net
- > os updates
- > os
- > password expiry
- ssh: disable

Custom Properties:


- > Application
- > Asset
- > Device
- > Host
- > LOB
- > Location
- > Security
- > Securit
- > Config
- > Adapter

- The **Edit Properties** pop-up appears as shown below:

Edit Properties - ZIGICAM_001 - 555cf103-7374-4dcf-a776-26df165b31c9

City	None	 
Campus	None	 
Building	None	 
Floor	None	 
Room	None	 
Username	root	 
Password	 

Name *

url 

Value *

163.123.2.9

Sensitive Property ☐

DONE **CANCEL**

+ Add

CANCEL **SAVE**

9. Add new values or modify existing values for Custom properties as required.

Note: You can find the list of Custom properties essential for enrolling the device, in the Adapter documentation or the Thing template's description. For assets connected via a TCP/IP network, these would be **IP Address**, and login credentials.

10. Click **Save**.

In a few minutes, you can see the Adapter running at the Edge connects with the newly registered Thing based on the Custom properties and **Enroll** the same.

You can also see the Thing's status change from **REGISTERED** to **ENROLLED** indicating that you've successfully onboarded the device.

7.2 Registering Things in Bulk

To register Things in bulk, perform the following steps:

1. Under **Inventory - Assets**, click the desired gateway.
2. Next, click the **Connected Assets** tab, and click **BULK REGISTER ASSETS**. The following wizard appears:
3. Select the desired device template from the drop-down menu, review the list of custom properties, and click **NEXT**. The following page appears:

Bulk Register Assets

- 1 Asset Template
- 2 Upload Asset Details**
- 3 Summary

Upload Asset Details

To upload asset details [click here](#) to download the CSV template file.

Enter asset details and upload the CSV file as shown in the image below.

	A	B	C	D	E	F	G
1	Device-Name	Adapter-Camera-IP	Location-Country	Location-State	Location-City	Location-Floor	Device-Date-Deployment
2	TP-Link Tapo C200	183.37.194.135	India	Karnataka	Bengaluru	GF	01/01/2021
3	Qubo Smart Cam 360	192.168.0.90	United State	Utah	Salt Lake City	Third	
4	TP-Link Tapo C100	192.168.100.1	United State	Arizona	Phoenix		21/08/2021
5	Srihome SH025 camera	192.168.1.108	India		Delhi	FF	

Choose CSV file Intel NUC - Vrindavan_bulk-register.csv

- Download the **CSV** template file by clicking the highlighted area as shown above.
- Open the downloaded **CSV** template file in an appropriate application such as **Microsoft Excel**. You will see **Device Name** as the first column followed by columns with names matching the Custom properties defined in the Thing template you selected previously.

Note: The **Asset Name** is a mandatory field.
- For each of the assets that you would like to bulk register, enter its Name and the required Custom properties into the **CSV** file, one-per-row.

Note: You can find the list of Custom properties essential for enrolling the device, in the Adapter documentation or the Thing template's description. For assets connected via a TCP/IP network, these would be **IP Address**, and login credentials.
- Ensure to save the file to disk in its original **.CSV** format.
- Go back to the **Upload Asset Details** page and click **Choose File** to upload the **CSV** file.
- Click **NEXT**. The following **Summary** page appears:

Bulk Register Assets

- 1 Asset Template
- 2 Upload Asset Details
- 3 Summary**

Summary


Review details given below and proceed with Bulk Registration

Asset Template Name
Avigilon Camera

Parent Asset Name
Intel NUC - Vrindavan

Number of Assets - 1

START REGISTRATION



[BACK](#) [CLOSE](#)

- Review the information on the **Summary** page and click **START REGISTRATION**. The registration process takes a few seconds and on success, you are taken to the

Connected Assets tab which now displays all the newly registered Things.

11. Any data errors in the uploaded **CSV** file will be visible so that you can rectify them and retry the registration.

Using the information provided by you when you registered, the Adapter will connect to the Things over its supported protocol and enroll them onto INFER™. This process may take a few minutes, depending on the number of assets registered.

As a result, you can see that the status of the onboarded Things have changed from **REGISTERED** to **ENROLLED**.

7.2.1 Viewing Asset Information

To view the list of information pertaining to a selected asset, click on the ellipsis (...).

1. Click **Command** to view the list of commands associated with the selected Asset. You can refresh the Command History on the top of the table to refresh any re-enrollment of assets. And click **Send Command** to modify your commands for the selected asset. For more information on commands, see [Working with Assets](#).
2. Click **Alerts** to view the alerts associated with the selected Asset.
3. Click **Files** to view the files, its size and the modification date of each file in a asset.
4. Click **Audit Log** to view the log of a specific asset.
5. Click **Campaigns** to view the associated Campaign of the selected asset from the list. Here, you can view the Campaign status and the State of a Campaign at that selected time.
6. Click **Certificates** to view the certificates of the selected asset.
7. Click **Vulnerabilities** to view or track the vulnerabilities of an asset. You can investigate incidents related to an asset, check the firmware version that contains the vulnerability fix, severity score of a vulnerability. You can click on the link under the **Vulnerability** column to know more information.

8 Spaces

This chapter explains spaces, and lists steps to create, edit spaces and assign parent spaces to space templates.

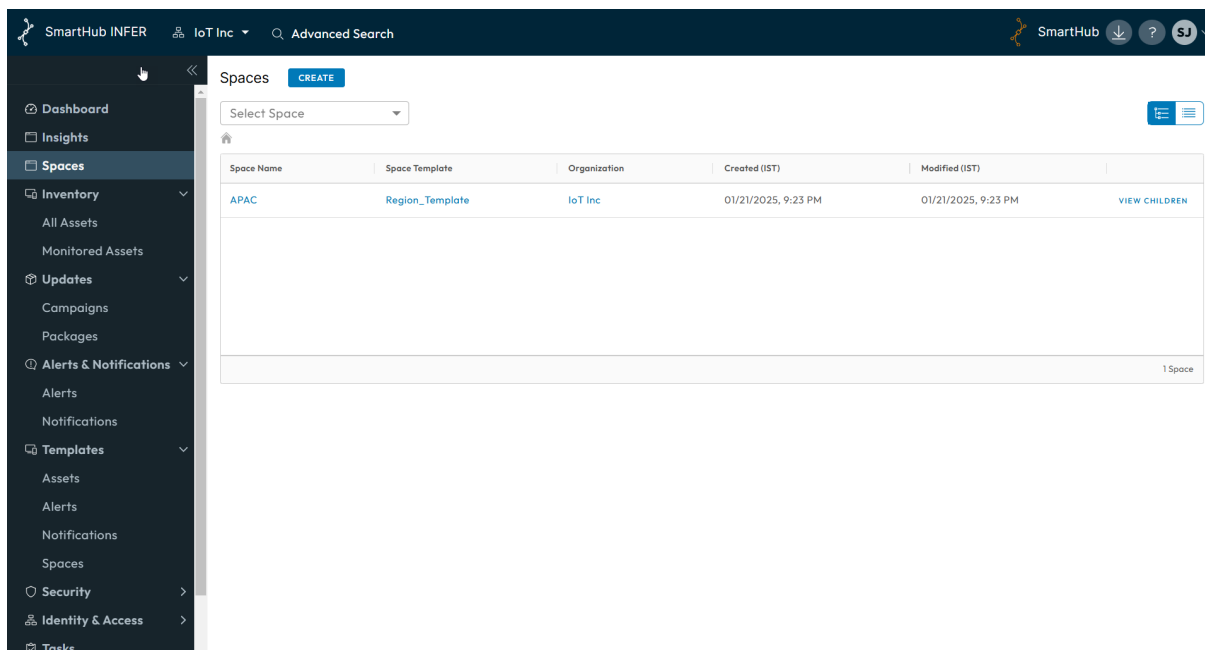
Spaces in INFER™ typically refer to the environments or contexts where IoT assets are deployed. These spaces can vary widely, from homes and offices to industrial settings and smart cities.

8.1 Creating Spaces

The concept of Space involves integrating IoT assets into specific spaces to gather data, enable automation, and enhance overall efficiency.

Prerequisite: To create a new space in INFER™, you must have the `CREATE_SPACE` permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ UI, navigate to **Spaces**. The **Spaces** page appears.
2. Click **CREATE**. The **Create Space** wizard appears.
3. Under **Space Template**, select the desired template from the drop-down menu.
4. Under **Display Name**, enter a valid name for the space template you are creating.
5. Select **Parent Space** and click **NEXT**. The attributes from space template is displayed.
6. Under **Space Attributes**, click the **Edit** icon to modify values of default attributes.
7. Click the **+ Add** icon and under **Name**, enter the new attribute's name.
8. Under **Value**, from the drop-down menu, enter the attribute's value and click **DONE**.
9. Under **Review**, review the space information you entered and click **SAVE**. You have successfully created a space.
10. You can now view your space in the **Spaces** page as shown below:



8.2 Editing Spaces

Prerequisite: To edit an existing space in INFER™, you must have the EDIT_SPACE permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ UI, navigate to **Spaces**. The **Spaces** page appears
2. From the listed spaces, click the space you desire to edit.
3. Under **Actions**, from the drop-down menu, click **Edit**.
4. The **Edit Space** wizard appears.
5. Select the Parent Space from the populated space tree as per its location. Click **Next**.
6. Under **Space Attributes** and click **+Add**, enter the Attribute name, Value name and click **Done**. Click **NEXT**.
7. Under **Review**, review the information and click **SAVE**. You have successfully edited a space.

8.2.1 Viewing Parent Space

With INFER™, you can view space hierarchy for a selected parent space on the Templates - Spaces page.

1. On the INFER™ UI, navigate to **Spaces**. The **Spaces** page appears
2. On the **Spaces** page, select a space from the drop-down menu.

The Space hierarchy allows you to drill down to the required space by clicking on any of the sub spaces listed for a parent space.

8.3 Assigning Spaces to assets

Assigning spaces to assets in INFER™ refers to the physical allocation of locations or areas where the assets are deployed based on the unique requirements and objectives of your edge infrastructure. This process involves carefully deciding where each asset should be positioned to optimize their performance, connectivity, and overall effectiveness in your edge network.

The goal is to ensure that each asset can efficiently communicate with other assets, gateways, or the central cloud system while also collecting accurate data from their surroundings.

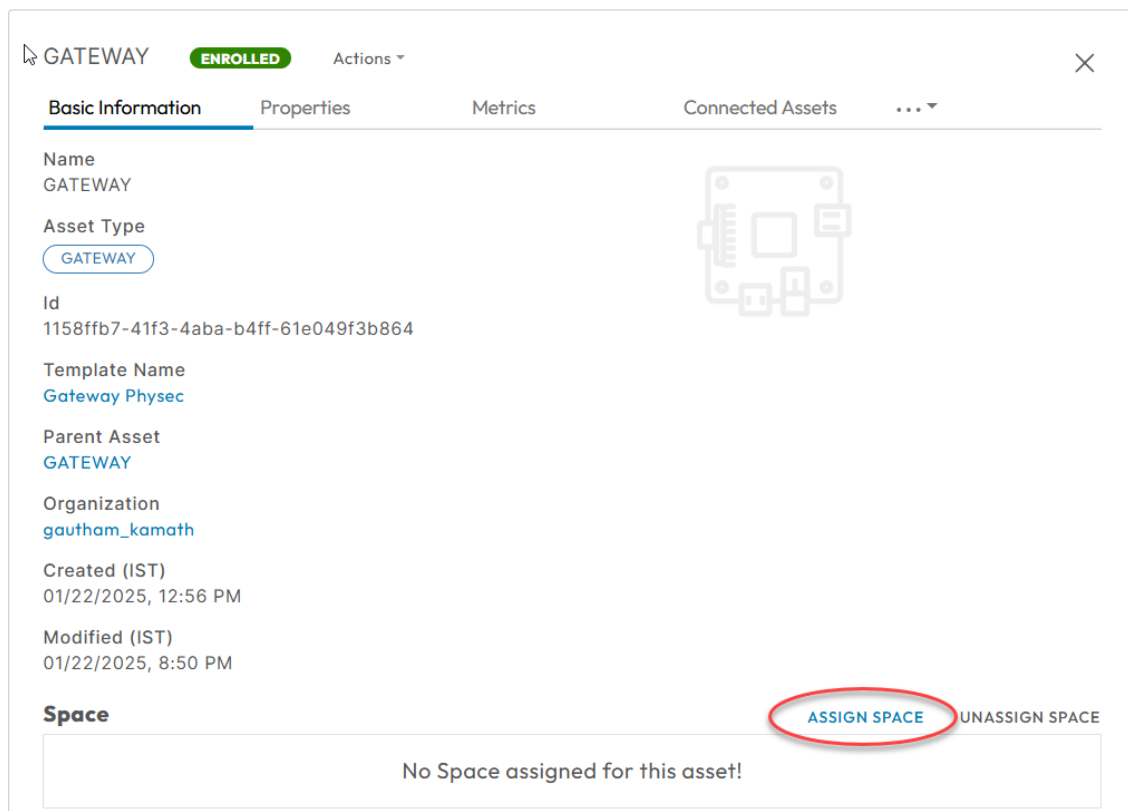
Listed below are some factors you want to consider before assigning spaces to assets:

- **Coverage and Connectivity:** Ensure that each asset has sufficient coverage of the area it needs to monitor or control. The assets should be positioned to maintain strong and reliable connectivity to the network, especially if they rely on wireless communication.
- **Line of Sight:** In scenarios where assets use radio frequency-based communication, for example, Wi-Fi, Bluetooth, Zigbee, it's essential to consider potential obstacles that may obstruct the signal. Avoid placing assets in areas with significant physical obstructions that could hinder communication.
- **Power Supply:** As assets require a stable power source, you can ensure that assets located in remote or hard-to-reach locations have easy access to power or use battery-powered assets with suitable battery life.
- **Environmental Conditions:** Consider the environmental conditions (e.g., temperature, humidity, exposure to elements) that each asset can withstand. Assets placed in extreme environments may require additional protection or specialized enclosures.

- **Data Collection Requirements:** Understand the specific data collection requirements of each asset and position them in locations that offer relevant data insights.
- **Redundancy and Resilience:** Plan for redundancy and resilience by deploying multiple assets in critical areas. Redundancy can help maintain continuous operation even if some assets fail.
- **Security and Privacy:** Be mindful of the security and privacy implications of asset placement, especially in sensitive environments. Avoid placing assets in locations where they can be easily tampered with or accessed by unauthorized individuals.
- **Scalability:** If your edge network is expected to grow over time, consider the scalability of the placement strategy to accommodate additional assets.
- **Maintenance and Accessibility:** Ensure that assets are easily accessible for maintenance, updates, and replacements when needed.
- **Data Transmission Latency:** For time-sensitive applications, consider the data transmission latency when deciding on the placement of assets. Minimizing latency can be crucial in certain IoT use cases.

Prerequisite: To assign a space to assets in INFER™, you must have the `EDIT_SPACE_TEMPLATE` permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ dashboard UI, navigate to **Inventory > Monitored Assets**.
2. From the listed assets, click the asset you desire to assign a space. The asset information appears as shown below:



3. Click **ASSIGN SPACE**. The **Assign Space to Asset** pop-up appears as shown below:

Assign Space to Asset

Asset Name: **172.17.0.4 AXIS Camera 4-digit Series**

▼ India

> Bengaluru

▼ United States

> Washington

> San Francisco

> Sanjose

> Seattle

> Palo Alto

▼ Ottawa

▼ Lion Building

> 1st Floor

> 3rd Floor

> Campus change

[CANCEL](#)[ASSIGN](#)

4. Locate and select your desired space under the root location, and click **ASSIGN**. You have successfully assigned a space to an asset.
5. Resultantly, as highlighted below, you can also see the breadcrumb navigation link showing the newly-assigned space's current location in your enterprise infrastructure:

avigilon camera **ENROLLED** Actions ▾

Basic Information Properties Metrics Connected Assets ... ▾

Name
avigilon camera

Asset Type
THING

Id
143776e2-566f-44cb-94d3-4fdb0ba3d038

Template Name
Avigilon Camera

Parent Asset
GATEWAY

Organization
gautham_kamath

Created (IST)
01/22/2025, 1:11 PM

Modified (IST)
01/22/2025, 4:08 PM

Space ASSIGN SPACE UNASSIGN SPACE

india > karnataka > bangalore > avigilon camera

8.4 Unassigning Spaces to Assets

Prerequisite: To unassign a space to assets in INFER™, you must have the EDIT_SPACE_TEMPLATE permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ dashboard UI, navigate to **Inventory > Monitored Assets**.
2. From the listed assets, click the asset you desire to unassign a space. The asset information appears as shown below:

192.168.20.106 AXIS Camera 4-digit Series **ENROLLED** Actions ▾

Basic Information Properties Metrics Connected Assets ... ▾

Name
192.168.20.106 AXIS Camera 4-digit Series

Asset Type
THING

Id
3da9feec-2bad-4f3b-8dae-a631fa468e5e

Template Name
AXIS Camera 4-digit Series

Parent Asset

Organization

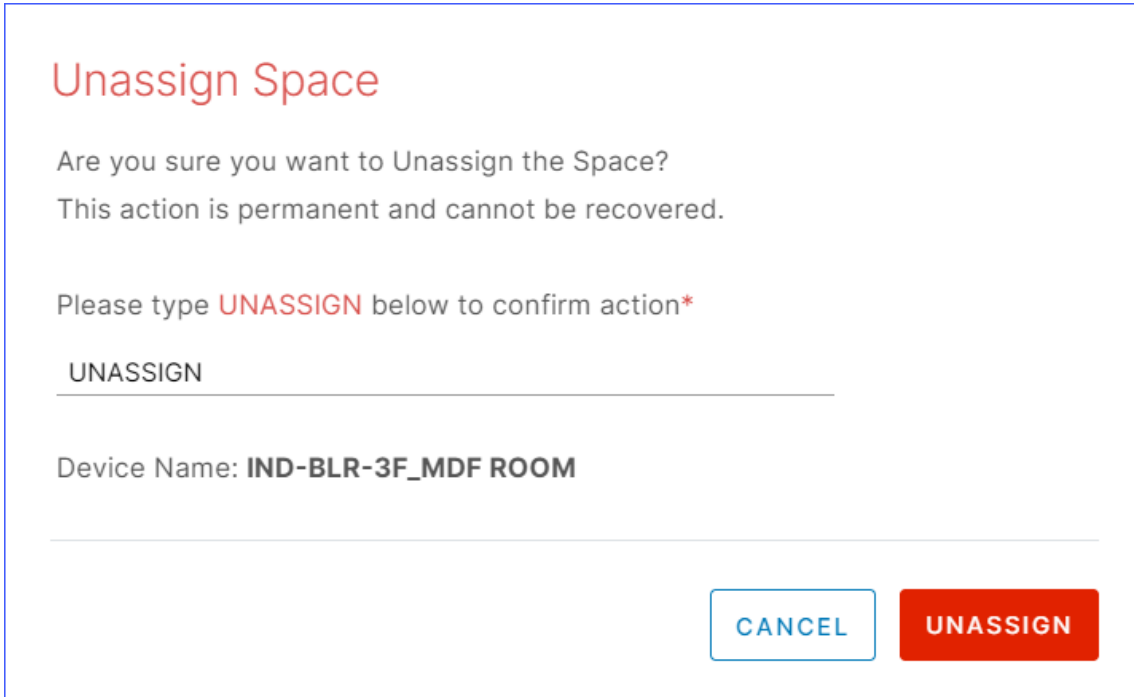
Created (IST)
09/05/2024, 7:57 PM

Modified (IST)
10/18/2024, 10:37 AM

Space ASSIGN SPACE **UNASSIGN SPACE**

India > Bengaluru > SmartHub Building > Floor 02 SmartHub > 192.168.20.106 AXIS Camera 4-digit Series

- Click **UNASSIGN SPACE** as highlighted above. The **Unassign Space** pop-up appears as shown below:



The image shows a 'Unassign Space' dialog box. At the top, the title 'Unassign Space' is in red. Below it, a message asks 'Are you sure you want to Unassign the Space?' and states 'This action is permanent and cannot be recovered.' A prompt asks the user to 'Please type UNASSIGN below to confirm action*'. There is a text input field containing 'UNASSIGN'. Below the input field, the 'Device Name' is listed as 'IND-BLR-3F_MDF ROOM'. At the bottom right, there are two buttons: a blue 'CANCEL' button and a red 'UNASSIGN' button.

- Enter **UNASSIGN** in the text area, and click **UNASSIGN**. You have successfully unassigned a space from an asset.

8.5 Assigning / Unassigning Parent Spaces

Space management in INFER™ operates on the concept of assigning a parent space to a space template and is associated with hierarchical or nested structures. The parent-child relationship helps organize and manage multiple interconnected spaces efficiently.

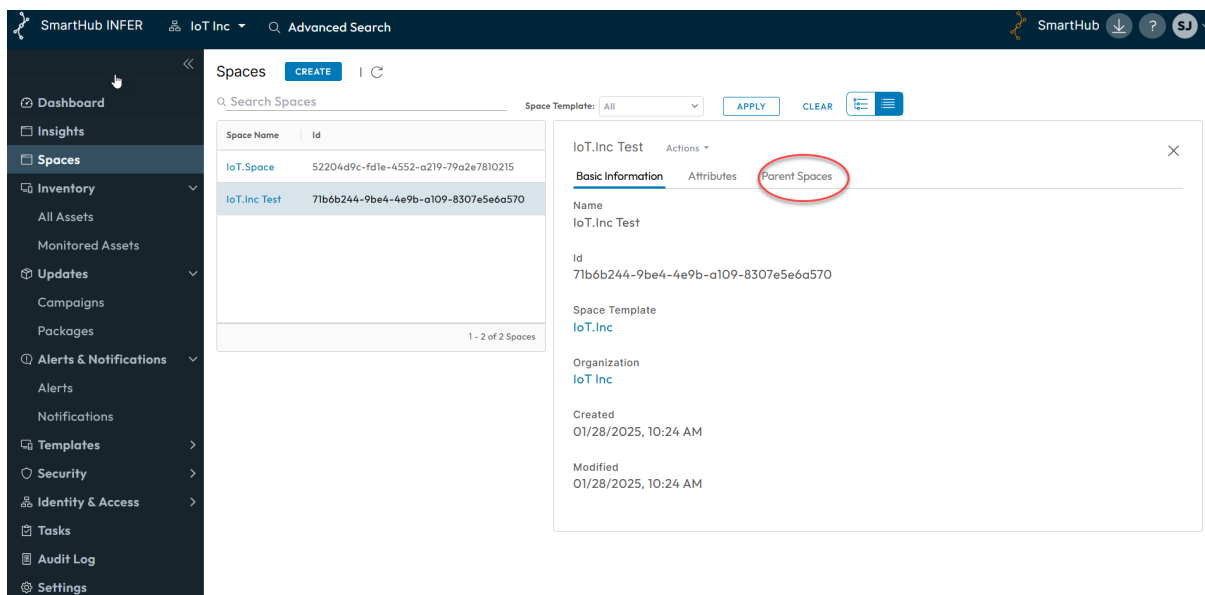
Listed below are some reasons why assigning a parent to a space template is important:

- Hierarchical Organization:** In INFER™, spaces can be structured hierarchically, such as a smart building containing multiple floors, each with various rooms or zones. Assigning a parent to a space template allows for logical grouping and easy navigation between spaces within the hierarchy.
- Consistency and Reusability:** A parent template in INFER™ encapsulates common features, configurations, or rules, ensuring consistency across all child spaces. Changes made at the parent level are propagated to all child spaces, enhancing maintainability and reusability of configurations.
- Centralized Control:** A parent template serves as a centralized control point for specific settings, such as energy management, security, or access control. This approach simplifies administration and updates since changes can be applied to the parent, affecting all associated child spaces.
- Granularity of Control:** With parent-child relationships, you can implement fine-grained control over different aspects of the spaces. For example, specific child spaces can have unique configurations while inheriting common characteristics from the parent.
- Scalability:** INFER™'s space templates allow for the expansion of the smart space infrastructure while maintaining an organized and manageable structure. For large-scale smart spaces, such as smart cities with multiple districts, neighborhoods, and buildings, the parent-child relationship enables scalable management.

- **Contextualization and Grouping:** Assigning a parent to an INFER™ space template allows you to contextualize spaces based on their functionality or location. You can group similar spaces together, facilitating better decision-making and data analysis.
- **Facilitates Data Aggregation:** When you have multiple child spaces, having a parent-child structure helps in aggregating data from different spaces for comprehensive analysis and reporting.

Prerequisite: As explained above, after creating the space template, to assign it to a parent space in INFER™, you must have the EDIT_SPACE_TEMPLATE permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ dashboard UI, navigate to **Spaces**.
2. From the listed spaces, click the newly-created space for which you desire to assign a parent space. The following tab appears as shown below:



3. Click the **Parent Spaces > Assign Parent Space**. The following pop-up appears:

Assign Parent Space

Space Name: **SafeSpaces HQ 1st Floor**

India

Bengaluru

SmartHub Building

SafeSpaces HQ

USA Region

CANCEL

ASSIGN

4. Locate and select your desired parent space under the root location, and click **ASSIGN**. You have successfully assigned a parent to a space template.

8.6 Bulk Assign Spaces to Assets

You can select multiple assets and assign to multiple spaces.

1. On the INFER™ dashboard UI, navigate to **Inventory > Monitored Assets**.
2. Select the checkboxes of your assets for which you want to assign spaces.
Note: Each page lists 20 assets. If no asset check boxes are selected, INFER™ auto-selects assets across all list pages.
3. Go to **Actions** drop-down menu > **Bulk Assign Space**. The **Bulk Assign Space** pop up appears as shown below:

Bulk Assign Space

×

✓ 4 Assets selected for Bulk assign Space.

Step 1 - Download Spreadsheet (.xlsx) containing Asset(s) details

DOWNLOAD SPREADSHEET

Step 2 - Edit Spreadsheet

- **Asset Name** in Green background are already assigned with Spaces
- Do not Delete/Edit existing Column headers
- Do not modify any columns except **Space**
- **Asset Id** and **Space Id** is kept hidden
- Modify **Space** using dropdown

Step 3 - Upload the updated Spreadsheet

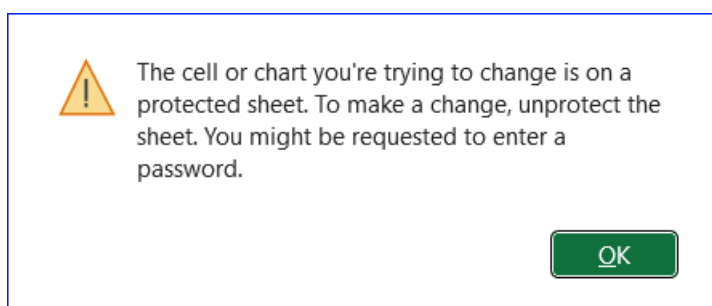
Drag and drop or click here to upload the .xlsx file

ASSIGN

- Next, click **DOWNLOAD SPREADSHEET** to download the spreadsheet (`bulk-assign-space.xlsx`).
- Open the spreadsheet to view the details of assets you selected.

Note:

- **Asset Id** (column A) and **Space Id** (column E) are kept hidden on purpose.
 - Do not modify any columns except Space.
 - Assets in Green background are already assigned with spaces. However, you can reassign them to different spaces.
 - Do not delete/edit existing column headers.
- If you attempt to modify existing column headers, the following error message appears:



8.6.1 Modifying Spaces

- Under **Space** column, click against any asset to pull the drop-down menu and select desired space.

2. After you complete assigning spaces to assets, save the file to disk in its original **XLSX** format.
3. Drag and drop the **XLSX** file in to the marked area or click the area as shown below:

Step 3 - Upload the updated Spreadsheet

bulk-assign-space.xlsx

×

Drag and drop or click here to upload the .xlsx file

ASSIGN

4. Click **ASSIGN** to bulk assign spaces to assets.

8.7 Deleting Spaces

Prerequisite: To delete an existing space in INFER™, you must have the DELETE_SPACE permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ UI, go to **Spaces**. The **Spaces** page appears.
2. From the listed spaces, click the space you desire to delete. **Note:** You can cannot delete more than one space.
3. Under **Actions**, from the drop-down menu, click **Delete**.
4. The **Delete Space** pop-up appears as shown below:

Delete Space

This action is permanent and cannot be recovered.

Do you really want to delete this space used by **27** asset?
Enter **DELETE** below to confirm action*

DELETE

Space Name: **India**

CANCEL DELETE

5. Enter **DELETE** in the text area, and click **DELETE**. You have successfully deleted a space.

Note: If the selected space is already associated with a child space, deletion will not occur.

9 Working with Insights

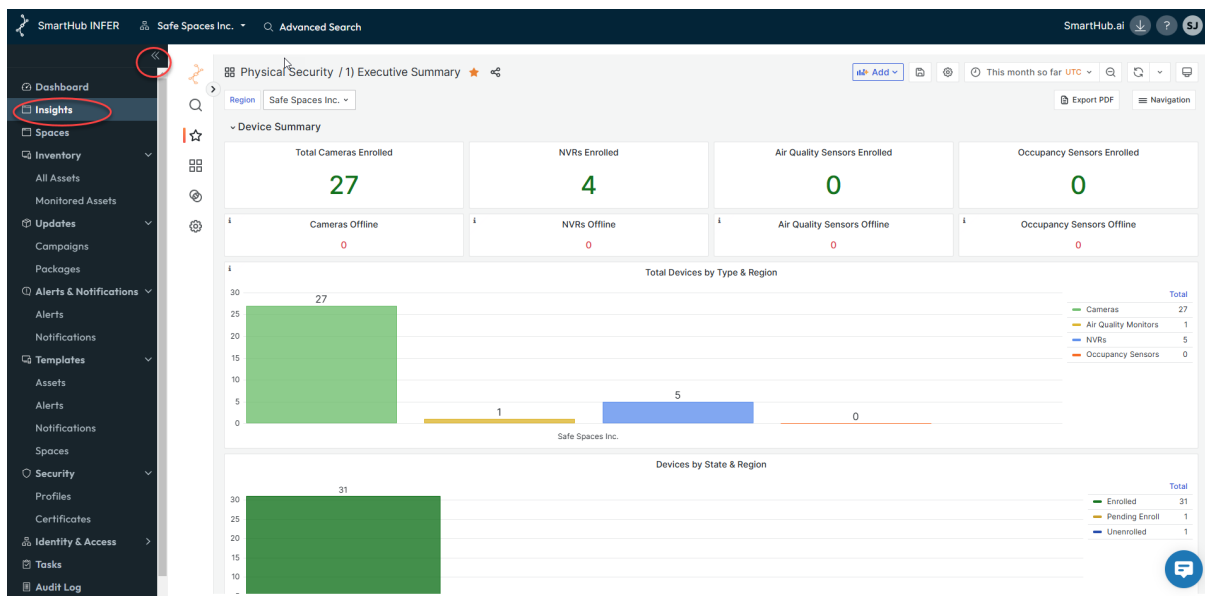
This chapter provides an overview of data visualization, monitoring, and data analysis capabilities of INFER™'s Insights module, and describes how to use dashboard search.

INFER™'s Insights dashboard is a visual interface of one or more panels arranged into one or more rows. It has a wide choice of panels making it easy for you to construct the right queries, and customize the visualization so that the perfect dashboard for your need can be created. Each panel interacts with data from any of INFER™ data sources configured by your administrator.

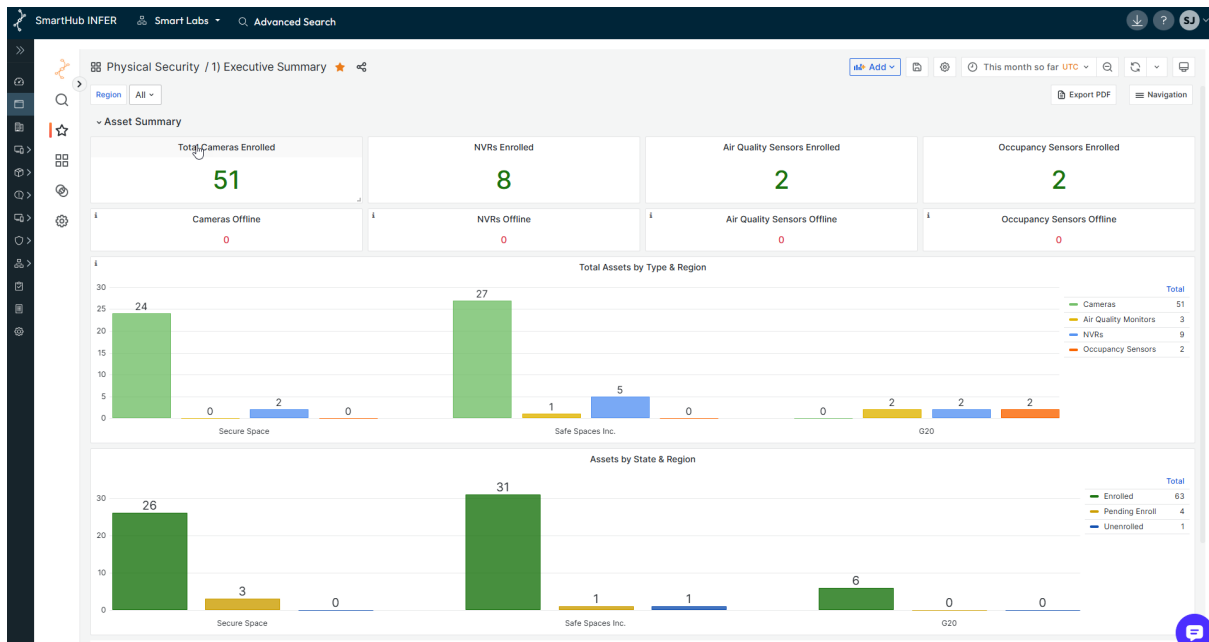
9.1 Viewing Dashboards

Prerequisite: To view INFER™'s Insights dashboards, you must have the IN-SIGHTS_VIEWER permission associated with the Organization Administrator Group.

1. On the INFER™ UI, navigate to **Insights**. The default **Executive Summary** page appears as shown below:



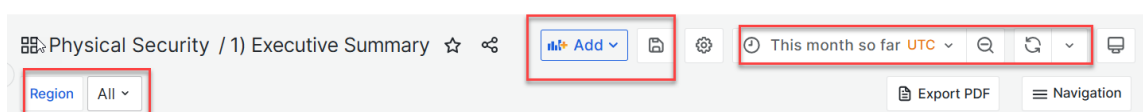
2. For expanded Insights page view, click the highlighted icon to collapse the left navigation bar. The full-width Insights page appears as shown below:



3. Under **Asset Summary**, as you scroll down, you can see various clickable panels showing the assets' vital performance indicators, and also list the following dashboards under it:
 1. **KPI (Time Filtered, Critical Alerts)**
 2. **Active Alerts Summary**
 3. **Firmware Summary**
 4. **Assets Need Attention**
4. Alternately, you can also click **Navigation** on the top right to list and access all dashboards available for your organization, as shown below:

- 2) Geo Map
- 3) Alerts Summary
- 4) Firmware Change Summary
- 5.1) All Models, Firmware & Vulnerabilities
- 5.2) Vulnerability
- 6) Asset-Cameras
- 7) Asset-NVRs
- 8.1) KPI - Uptime
- 8.2) KPI - MTTR
- 8.3) KPI - MTBF

5. To perform a more focused analysis of any panel, Insights provides you the following filters to work on any data set with hundreds of records:



6. To perform focused analysis on individual data sets, select **View** from the drop-down as shown below:

▼ Camera Settings

Key Network Settings for Cameras

Name	IP Address	SSH Enabled	RTSP	View	Enabled	HTTP Enabled	HTTPS Enabled
Axis Q3515 LV IND BLR SH 192.168.29.4	192.168.29.4	no	yes	ⓘ Edit			
Axis-Physic-Lab	192.168.29.4	yes	yes	🔗 Share			
Dell Demo May 30th	192.168.29.4	no	yes	🔍 Explore			
GP-Test-Camera March 15th	10.42.0.121	no	yes	🔍 Inspect			
IND-BLR-3F_ENTRY ROOM	115.31.187.247	no	yes	⋮ More...		yes	yes
IND-BLR-3F_IDF ROOM	75.37.239.39	no	yes	🗑 Remove	no	yes	yes

7. The following view appears making it easier for you to work the panel data set within a dedicated view along with filters:

Physical Security / Cameras

Region All Country All City All Building All Floor All Camera All

Key Network Settings for Cameras

Name	IP Address	SSH Enabled	RTSP Enabled	FTP Enabled	HTTP Enabled	HTTPS Enabled
Axis Q3515 LV IND BLR SH 192.168.29.4	192.168.29.4	no	yes	no		
Axis-Physic-Lab	192.168.29.4	yes	yes	no		
Dell Demo May 30th	192.168.29.4	no	yes	no		
GP-Test-Camera March 15th	10.42.0.121	no	yes	no		
IND-BLR-3F_ENTRY ROOM	115.31.187.247	no	yes	no	yes	yes
IND-BLR-3F_IDF ROOM	75.37.239.39	no	yes	no	yes	yes
IND-BLR-3F_MDF ROOM	16.172.200.43	no	yes	no	yes	yes
IND-BLR-3F_MDF ROOM	209.251.46.146	no	yes	no	yes	yes
IND-BLR-3F_PF ROOM	158.140.89.235	no	yes	no	yes	yes
IND-BLR-4F_BALCONY	187.235.110.253	no	yes	no	yes	yes
IND-BLR-4F_DATA ROOM	62.103.178.205	no	yes	no	yes	yes
IND-BLR-4F_ENTRY ROOM	77.160.111.147	no	yes	no	yes	yes
IND-BLR-4F_EXIT STAIRS	104.80.86.155	no	yes	no	yes	yes
IND-BLR-4F_IDF ROOM	242.54.101.243	no	yes	no	yes	yes
IND-BLR-4F_LIFT AREA	26.116.191.69	no	yes	no	yes	yes
IND-BLR-4F_MDF ROOM	187.243.83.137	no	yes	no	yes	yes

9.1.1 Exporting to PDF

You can export your dashboard data directly to PDF by performing the following steps:

1. Click the **Export PDF** icon to open the **Executive Summary** dashboard data in PDF format (`Executive Summary.pdf`) in a new tab for the chosen time range.

9.2 Customizing Dashboards

To customize the presentation of your data, the Insights module's dashboard provides several user interface elements as listed below:

1. Time settings are saved on a per-dashboard basis.
2. **Zoom out time range:** Click the **Lens** icon to zoom out the time range.
Note: The dashboard and panel time controls have a common Console.
3. **Refresh dashboard:** Click the **Refresh** icon to immediately run every query on the dashboard and refresh data and visualizations.
By default, Insights does not automatically refresh the dashboard. Queries run on their own schedule according to the panel settings.
4. **View Mode:** Click the **TV mode** icon to display the dashboard on a large screen such as a TV or a kiosk.

Note: View mode hides irrelevant information such as navigation menus.

5. **Starred dashboards:** Starred dashboards help you remember to view them later within Insights. You can mark your favorite dashboards by clicking the **Star** icon of any listed dashboard and change its color to **Orange Star**.

9.2.1 Setting Absolute Time Range

You can set an absolute time range in the following ways:

Absolute time range

From

To

Apply time range

- Last 24 hours
- Last 7 days
- Last 30 days
- Last 90 days
- Last 6 months**
- Last 1 year
- Last week
- Previous month
- This month so far

Coordinated Universal Time UTC, GMT UTC

1. Type your desired values into the **From** and **To** fields. You can type exact time values or relative values, such as `now-24h`.
2. Click **Apply time range**.
3. Click in the **From** or **To** field to display a calendar. Click the day or days you want to use as the current time range.

Note: UTC is set as a the **Coordinated Universal Time**.

4. Click **Apply time range**.

9.3 Downloading Data from Table Panels

The table panel offers many ways to manipulate your data for optimal presentation.

Using the panel inspect view, you can troubleshoot your panels. This option helps you to use all the available dashboard filters to focus deeply on a particular panel.

You can also inspect the raw data for any Insights panel and export that data to a `CSV` file.

Known Vulnerable Firmware, Support and Age

Cameras with Known Vulnerable Firmware

Model	Model Support Expiry Date	Total Cameras	Cameras with	Latest Firmware Version	Recommended Version
AXIS Q3515 Network Camera	2023-06-08	13		10.7.1	
AXIS P3245-LV Network Camera	2027-12-31	10		11.6.94	10.12.199
AXIS P3719-PLE Network Camera	2024-05-28	5			10.12.199

1 - 3 of 3 rows

Camera Firmware Age

Model	Total Cameras	Cameras on Latest Firmware	Firmware Age less than 2 years	Firmware Age 2 to 5 years	Firmware Age more than 5 years
AXIS P3245-LV Network Camera	10	0	10	0	0
AXIS P3719-PLE Network Camera	5	0	2	3	0

1. To download data from any panel, open the panel menu and go to **Inspect > Data** as shown above.
2. The following side page appears:

Inspect: Cameras with Known Vulnerable Firmware

3 queries with total query time of 1.17 s

Data Stats JSON Query

> Data options Formatted data Download CSV

Model	Model Support	Total Cameras	Cameras with	Latest Firmware Version
AXIS Q3515 Network Camera	2023-06-08	13	7	10.7.1
AXIS P3245-LV Network Camera	2027-12-31	10	8	11.6.94
AXIS P3719-PLE Network Camera	2024-05-28	5	5	11.6.94

3. Click **Download CSV** to download the CSV file.

10 Working with All Assets

This chapter explains INFER™'s Asset module and lists steps to manage your IoT device assets across the enterprise.

Building and maintaining a well-organized IoT asset database is critical for effective asset management, security, and operational efficiency in industrial and enterprise IoT deployments. It serves as a centralized source of information for decision-making, troubleshooting, and optimizing the performance of IoT devices. However, managing your IoT assets using manual systems can be inefficient and prone to errors.

INFER™'s Asset ledger is a structured and organized database of device asset information within your edge network. This database plays a crucial role by helping your IoT crew maintain up-to-date IoT device asset data, monitor device life cycle status, improve their operational efficiencies, security, and generate insights.

It automatically discovers and classifies every single device, including those not registered in INFER™, complete with high-fidelity information such as make, classification, location, and application/port usage and displays them in the Asset Ledger.

Post discovery, gives you real-time, continuous visibility of the single source of asset inventory truth throughout their myriad life cycles. This enables you to distinguish each IoT device from all others for risk mitigation areas like:

- Vulnerability management
- Access management
- Data protection
- Incident detection

This information can also be integrated into Information technology Service Management (ITSM), Configuration Management Database (CMDB), and Computerized Maintenance Management System (CMMS) solutions.

The Asset Ledger module enables you to capture IoT asset data within folders and monitor your device deployments.

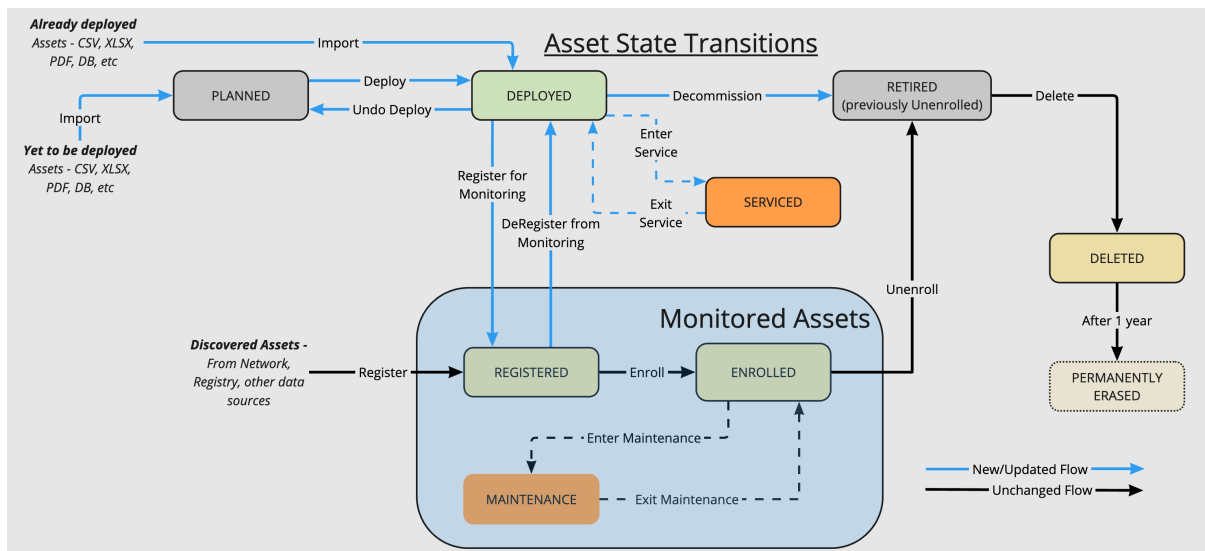
- Manage both tangible and in-tangible assets: This can include monitored and non-monitored assets.
- Provides an ability to track any number of properties for every asset.
- Provides a view with a list of assets on a page with the ability to filter by various attributes of the asset.
- Provides users to edit the properties of one or more assets.
- Provides an ability to associate an Asset to a Space.
- Provides a method to change the state of one or more assets.
- Provides a built-in Asset Insights Dashboards.

10.0.1 Asset State Transitions

These are the various states that an Asset can be in:

- Planned - Assets that are planned to be procured or in procurement (but are not yet deployed). These could be imported into INFER™ as Excel/PDF files or other sources like ERP, Purchasing systems, databases.
- Deployed - Assets that are already deployed (post procurement) but are not enabled for monitoring. These could be imported into INFER™ as Excel/PDF files or other sources like ERP, Purchasing systems, databases.

- Assets that have the ability to communicate and are being monitored by INFER™. The following are the sub-states of an asset:
 - Registered - Ready to be enrolled for monitoring
 - Enrolled - Enrolled for monitoring and being actively monitored
 - Maintenance - Temporarily under planned downtime for maintenance (No new Alerts are generated)
- Under Service - Being serviced either on-site or sent off-site to a vendor.
- Retired - When an asset is in the process of getting de-commissioned.
- Deleted - When deleted, an asset will be kept in the database for up to 1 year before getting wiped permanently.



10.1 Adding Assets

- On the INFER™ UI, navigate to **Inventory > All Assets**. The **All Assets** page appears as shown below:
- Click the vertical ellipsis and click **+ Add Assets**.

The dialog box titled **How would you like to add Assets?** presents three options:

- Add Single Asset:** Add a single asset for a particular template.
- Add Multiple Assets:** Add multiple assets for a particular template.
- Import from a predefined format:** Upload a file in the supported format to add assets.

At the bottom, there are **Cancel** and **Continue** buttons.

- For a single asset, click **Add Single Asset > Continue**:
 - On the **Add Single Asset** page, enter a valid **Asset Name**.
 - Select an existing asset template from the **Asset Template** drop-down menu.

3. If your asset is in Deployed or Planned state, select either of them under the **Initial Asset Status** drop-down.
4. If you have selected *Deployed*, then you have an option to assign a Parent asset to the selected Thing asset. Note that this option is only available for a Thing asset.
5. Click **Review**.
6. Once you review your asset details, continue to add by clicking **Add**.

Add Single Asset

Asset Name
LKH_HR 11_T

Asset Template ⓘ
Trio

Initial Asset Status ⓘ
Deployed

Parent asset (Optional) ⓘ
HD404031 - Copo Zoom-Room

← Back Review

4. For multiple assets, click **Add Multiple Assets > Continue**:
 1. On the **Add Multiple Assets** page, select an existing template from the **Asset Template** drop-down menu.
 2. Click the *Download XLSX template to fill* to download the XLSX file on your local machine.
 3. Enter the Asset details in the XLSX file and under the **Upload Assets** section, select your file to upload all your asset information.
 4. If your asset is in Deployed or planned status, select either of them under the **Initial Asset Status** drop-down.
 5. If you have selected *Deployed*, then you have an option to assign a Parent asset to the selected Thing asset. Note that this option is only available for a Thing asset. Click **Review**.
 6. Once you review your asset details, continue to add by clicking **Add**.

Add Multiple Assets

Asset Template ⓘ

MacMini Test Gateway 1

Download XLSX template to fill

Upload Assets ⓘ

Drag & drop .xlsx file to upload assets

Maximum File Size : 18 MB

Select File

Initial Asset Status ⓘ

Planned

← Back Review

5. To import assets, click **Import from a predefined format > Continue**.

1. On the **Import from a predefined format** page, select a file format from drop-down menu.
2. Under the **Upload Assets** section, select your file to upload all your asset information.
3. If your asset is in Deployed or planned status, select either of them under the **Initial Asset Status** drop-down.
4. If you have selected *Deployed*, then you have an option to assign a Parent asset to the selected Thing asset. Note that this option is only available for a Thing asset. Click **Review**.
5. Once you review your asset details, continue to add by clicking **Add**.

Note - The file format transforms raw data from an Excel workbook containing various asset details for import into the INFER™ platform. To enable this file format on INFER™, ensure a package labeled *DTA* is already uploaded to the platform. For more details, refer to the Package section or contact SmartHub Support.

4. Under **Upload the xlsx File**, drag and drop the `xlsx` file you are creating. This `xlsx` must carry relevant asset columns as highlighted in example shown below:
 5. Under the **Initial Asset Status** drop-down menu.
- Note:** For more information on Asset State, see [Asset State Transitions](#).
6. Click **Review** and click **Add**. You can then view a list of assets.

10.1.1 Search an Asset

1. Under the **All Assets** page, click the Search icon to enter your asset.

10.1.2 Filter an Asset

You can filter an asset based on its Template, State and Location.

1. On the **All Assets** page, navigate to **Filters**.
2. Click on any of the option that is listed under it.
 - The template lists all *Asset Templates* existing on the INFER™ UI.
 - State implies the state of a selected asset. For example, you can filter an asset based on its Deployed, Registered, retired state etc.
 - Asset Type provides the type of Asset whether is is a Gateway or a Thing.
 - Location implies the exact deployed location of an asset.

10.2 Understanding Asset Information

1. Click on any assets under the **All Assets** page.
2. Under the **Basic Information** tab, you can view the high-level information pertaining to the asset. The page provides you with information like, Asset ID, Name, State, Asset Type, Organization, Space and last modified information.

You can also click **Change State** to change the state of an asset.

3. Under the **Properties** tab, you can view a list of defined **System Properties** and **Custom Properties**.
4. Under the **Metrics** tab, you can view the metrics graphs. For more information on understanding System and Custom Properties, see [Working With an Asset as a Template](#) section.
5. The **Command** tab provides a list of commands that are associated with each assets with further information like Command Name, Type and the argument of each command. For a File Upload command type, you can even Download the file under the **Response** column.

← Back to All Assets

HD404031 - Copo Logitech Rally Bar

- Basic Details
- Properties
- Metrics
- Commands



Asset Information

Asset ID	80227fff-3c39-49c8-8821-f807d3e42aa1	Copy
Name	HD404031 - Copo Logitech Rally Bar	Edit
State	ENROLLED	Change State
Asset Type	THING	
Template	Logitech Rally Bar	Link
Organization	Converge	
Space	NASA ► Costa Rica ► Heredia ► C-11 ► C-11-4th Floor ► HD404031 - Copo	
Last Modified At	Apr 29, 2025, 5:26 PM	

10.2.1 Edit a Property

1. On the Asset page, expand the Properties by clicking **+Expand All**
2. Select any property and click on the **Edit** icon. The **Edit Property** wizard opens on the right hand side of the window.
3. You can edit the Name and value of the property and click **Save Changes**.




Properties (21)

- Adapter
 - Crestron
 - PORT 22
 - Refresh
 - Cycle 5
 - HOST 127.119.36.213  
 - PASSWORD Flr3Fli!
 - USER user
 - Smartspaces
 - Location
 - Device
 - Asset
 - Room

Edit Property

Name: Adapter-Crestron-HOST

Value: 127.119.36.213

10.2.2 Delete a Property

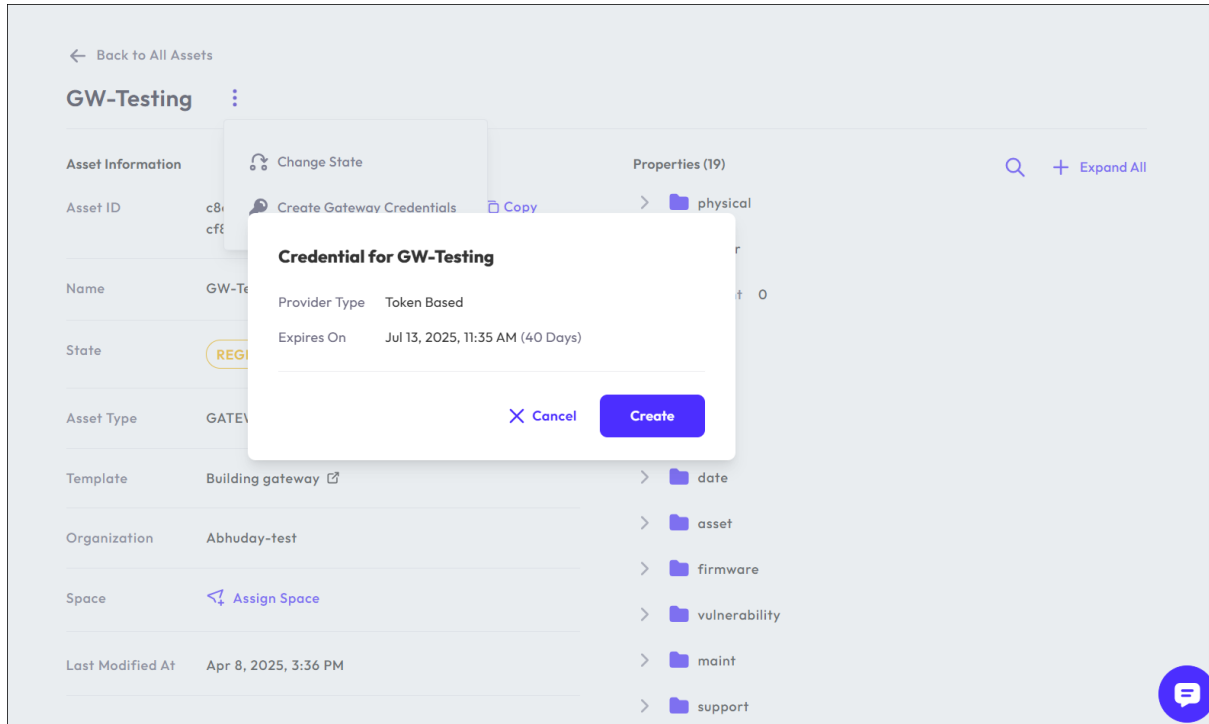
1. On the Asset page, expand the Properties by clicking **+Expand All**
2. Select any property and click on the **Delete** icon. The **Confirm Deletion** wizard appears.
3. Click **Delete** after you confirm the action.

10.2.3 Adding Gateway Credentials

You can create a gateway credential for an asset on the All Assets page.

Pre-requisites

- Verify that an asset is a gateway.
- Verify that an asset is either in *Registered* or in *Maintenance* state.



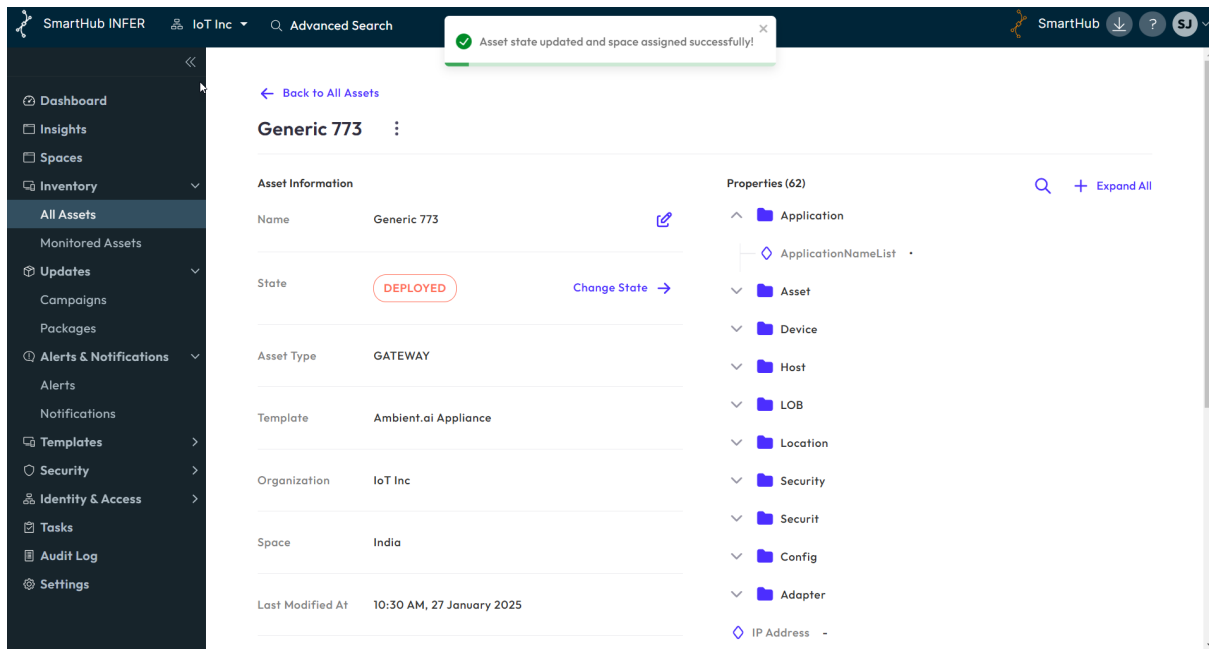
Note: Creation of credentials could either be Property based or Token based depending on the enrolment provider configured for the asset

1. On the **All Assets** page, select an asset that is a gateway that is already registered or in maintenance state.
2. Click on the vertical ellipsis, click **Create Gateway Credentials**.
3. For a token-based enrollment, click **Create** and copy the Credential. Click **Finish**.
4. For a property-based enrollment, enter the value and click **Submit**.

10.2.4 Change the State of an Asset

You can change the state in three different ways.

1. You can navigate to the three vertical ellipsis on the **All Assets** page and click **Change Status**.
2. Click on an Asset and on the Asset page, click **Change State**.
3. Select the Asset on the **All Assets** page and click the vertical ellipsis. Click **Change Assets**.



10.2.5 Update Agent

You can upgrade your agent installed on a particular asset to the latest version that is available.

1. Click on any asset.
2. On the asset page, navigate to vertical ellipsis.
3. Click **Update Agent**
4. Click **Confirm** to confirm the version update.

10.2.6 Edit an Asset Name

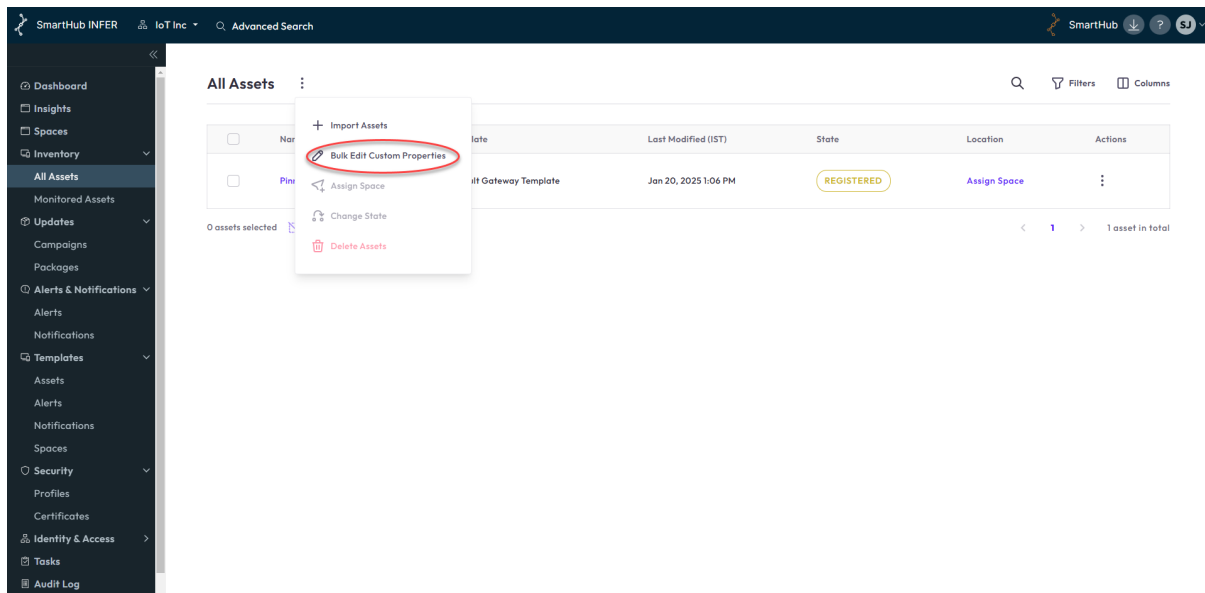
1. You can edit a name of an Asset, by clicking the Asset on the **All Assets** page.
2. Click the Pencil edit icon.
3. Edit the name of the asset on the right hand window.
4. Click **Save**.

10.2.7 Search a Property

1. After you click on an Asset, the Asset page opens up. On the right hand side, enter the property that you are searching on the Search field.
2. The entered property is expanded accordingly.
3. You can click **+ Expand All** to view all the properties.

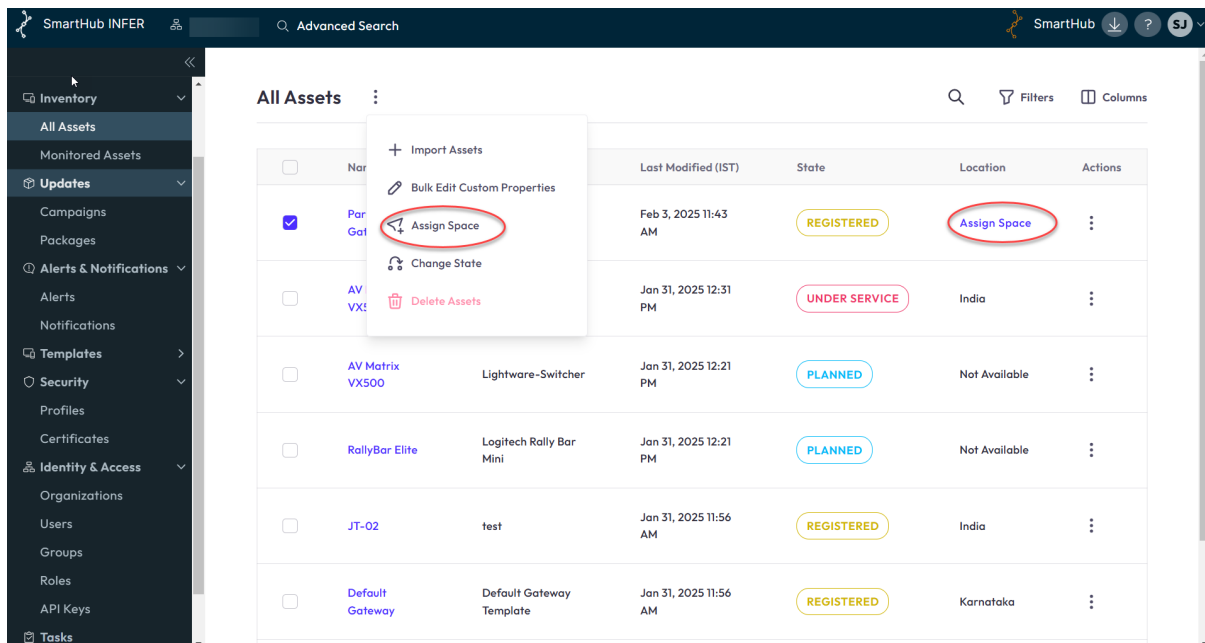
10.3 Bulk Edit Custom Properties

1. Navigate to All Assets and click the vertical ellipsis.
2. Select **Bulk Edit Custom Properties**.
3. After you edit the excel sheet locally, click **Select File** to upload the edited file.
4. Click **Submit**.



10.4 Assign Space

1. On the **All Assets** page, navigate to **Assign Space**. The **Assign Space to Asset(s)** wizard appears.
2. You either search an existing space or expand the space tree to select a specific Space.
3. Click **Assign**.



10.5 Connect to Parent

You can structure assets hierarchically, establishing parent-child relationships for better organization. This feature helps manage dependencies and connections between assets efficiently.

Each asset can have multiple child assets linked to a single parent. Note that the child device template must be linked to a parent device template.

Prerequisites

1. While requesting hierarchy creation, all selected assets must belong to the same template and be in the deployed state.
2. The selected asset's template must be a child template of another template; only then will it suggest parent devices for connection.
3. Once a child asset is attached to a parent, the user cannot reattach it to a different parent.

To connect a child device template to parent device template:

1. On the **All Assets** page, select any **Asset** and click **All Assets > Connect to Parent**. If the child template is already a child of the selected parent template then you will automatically view it in the drop-down menu.
2. Click **Confirm**.

Note

1. When changing an asset's state, you can select either standalone assets or assets linked to a parent, but not a combination of both.
2. To transition an asset (or multiple assets) from *Deployed* to *Registered*, the parent asset must be in the *Registered* state.

11 Working with Assets

This chapter details the assets' operational states and the various operations you can perform on them:

11.1 Sending Commands to INFER™ Agent

You can send a command to the Agent on your gateway from the INFER™ Console.

1. On the INFER™ UI, navigate to **Inventory > Monitored Assets**.

The **Inventory - Monitored Assets** page lists the **Asset Type**, **Template Name**, **Enrollment State** and **Connected Assets** of gateways and Thing assets.

2. Click the desired asset to which you want to send a command.
3. From the ... (3 dots) drop-down menu on the right, select **Commands > SEND COMMAND**.
4. In the **Send Command** pop-up window, from the **Select Command** drop-down menu, select the required command.
5. Under **Command Type**, enter its arguments.
Note: This command will run with root privilege.
6. Click **SEND COMMAND** to send the command to selected assets.
7. As a result, the status of the command appears under **Command History**. Click **Refresh** to refresh the status.

11.2 Sending Commands to Multiple Assets

You can send a command from the INFER™ Console to up to 1000 assets.

Note: The selected assets must belong to the same template.

1. On the INFER™ UI, navigate to **Inventory > Monitored Assets**.
2. Select the checkboxes against the assets for which you want to send a command.
3. Go to **Actions** drop-down menu > **Send Command**. The **Send Command** pop-up appears as follows:

Send Command

Asset: avigilon camera
Asset Template: Avigilon Camera

Select Command

Update User Password

Description

Command to change the camera password for...

Command Type

CLIENT_EXECUTE

Client Identifier

com.smarthub.avigilon.ai

Arguments

Username

-

password

-

CANCEL SEND COMMAND

- Under **Select Command**, from the drop-down menu, select the command.
- Click **SEND COMMAND** to send the command to the selected assets.
- As a result, the status of the command appears under **Command History**. Click **Refresh** to refresh the status.

Note: You can verify the status of the asset command update on multiple assets using the **Tasks** tab.

For more information, see [Tasks](#).

11.3 Bulk Command Cancellations

You can cancel asset **PENDING** commands in bulk on the INFER™ UI.

Presently, when you perform a command for a asset, this new command gets the default state as **PENDING**. Here, the asset's agent picks this new command for execution, and once completed it gets into the **EXECUTE** state.

In certain circumstances, the agent fails to pick your commands and they instead continue to remain permanently in **PENDING** state. This **PENDING** state also routinely stops you from performing many essential operations on that asset, for example, asset unenrollment.

1. On the INFER™ UI, navigate to **Inventory > Monitored Assets**.
2. Click the asset whose pending commands you want to cancel.
3. Click the ... (3 dots) drop-down menu > **Commands** to display the list of commands.
4. Select the checkboxes of desired commands showing **PENDING** status.
5. Next, click **CANCEL SELECTED COMMANDS**. The **Cancel Pending Commands** pop-up appears where you can review the commands you have chosen to cancel.
6. Under **Reason to cancel pending commands**, enter your reason.
7. Click **SUBMIT** to cancel the pending commands.

11.4 Asset States

INFER™ displays various operational states that assets can be in during their lifecycle. These states help in understanding and managing the asset's behavior and are relevant for asset management and monitoring purposes.

The five states for assets supported by INFER™ are listed below:

1. Registered
2. Enrolled
3. Unenrolled
4. Deleted
5. Maintenance

11.4.1 Viewing List of Assets by State

You can view the list of the assets based on their state such as enrolled, registered, unenrolled, and deleted.

You must be a **Asset Administrator** to perform this operation.

1. On the INFER™ UI, navigate to **Inventory > Monitored Assets**.
2. From the **Enrollment State: ...**, select the state and click **APPLY**.

The list of assets with the selected state is appears.

Note: If you want to view all the deleted assets, select the **Deleted** check box. **Deleted** check box is not selected by default. You can only view the basic information of the deleted assets.

11.5 Asset Maintenance

Asset maintenance in INFER™ refers to the ongoing tasks and activities performed to ensure the proper functioning, security, and longevity of assets throughout their lifecycle. Planned and effective maintenance is essential to prevent asset malfunctions, security breaches, and performance degradation.

11.5.1 What Happens to Assets in Maintenance?

When a asset is put into maintenance:

- Caches the asset state in the agent
- Stop alert generation
- Stores the reason in the audit log
- Collects any incoming metrics or any other data

Note: You can optionally change the state of the assets connected to a asset already in **MAINTENANCE**.

11.5.2 Entering Maintenance

Prerequisite: To put a asset into maintenance state in INFER™, you must have the `EDIT_DEVICE_STATE` permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ UI, navigate to **Inventory > Monitored Assets**. The **Inventory - Monitored Assets** page appears.
2. Click the checkbox against the desired asset.
3. Go to **Actions > Enter Maintenance**. The **Enter Maintenance** pop-up appears as shown below:

4. Under **Provide a reason for this change** enter your reason.
5. Next, select the checkbox if you want to **Auto-apply this change on children of the selected asset(s)**
6. Click **ENTER MAINTENANCE**. You have successfully put the selected things in **MAINTENANCE** state.

11.5.3 Exiting Maintenance

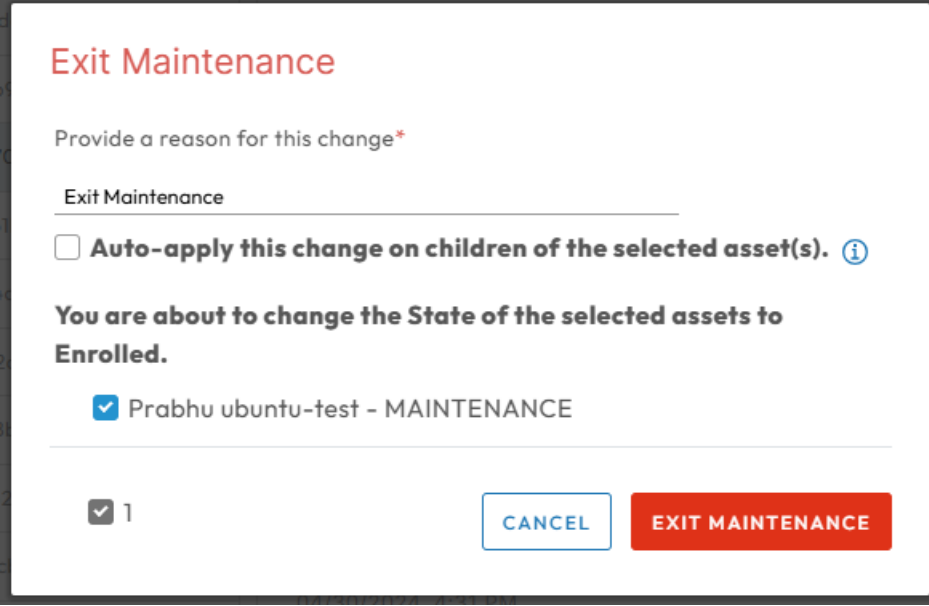
From the **MAINTENANCE** state, you can change the asset state to **ENROLLED**. When you invoke **Exit Maintenance**, you can notice the following possible changes:

- Changes the asset state to **ENROLLED**
- Caches the asset state in the agent
- Stores the reason in the audit log

- Invokes alerts

Prerequisite: To bring a asset out of maintenance state in INFER™, you must have the EDIT_DEVICE_STATE permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ UI, go to **Inventory > Monitored Assets**. The **inventory - Monitored Assets** page appears.
2. Click the checkbox against the desired asset in the list.
3. Go to **Actions > Exit Maintenance**. The **Exit Maintenance** pop-up appears as shown below:



The image shows a 'Exit Maintenance' dialog box. At the top, the title 'Exit Maintenance' is in red. Below it, a text prompt says 'Provide a reason for this change*'. There is a text input field containing 'Exit Maintenance'. Below the input field is a checkbox labeled 'Auto-apply this change on children of the selected asset(s)' with an information icon. A bold message states 'You are about to change the State of the selected assets to Enrolled.' Below this, a list shows one asset: 'Prabhu ubuntu-test - MAINTENANCE' with a checked checkbox. At the bottom left, there is a summary '1' with a checked checkbox. At the bottom right, there are two buttons: 'CANCEL' and 'EXIT MAINTENANCE'.

4. Under **Provide a reason for this change** enter your reason.
5. Next, select the checkbox if you want to **Auto-apply this change on children of the selected assets**
6. Click **EXIT MAINTENANCE**. You have successfully reverted the selected Things' state into **ENROLLED** state.

11.6 Asset Migration

In an enterprise IoT ecosystem, you may decide to move things between gateways due to various circumstances as listed below:

- **Network Coverage and Range:** If a Thing's current gateway is not giving sufficient network coverage or range due to physical barriers, signal interference, or limitations of the gateway's wireless technology, you may have to move the asset to another gateway with better coverage.
- **Load Balancing:** In situations where multiple gateways are deployed, assets may need to be moved between gateways to balance the network load. This ensures that the traffic and data transmission are distributed optimally among the gateways, preventing congestion and other performance issues.
- **Gateway Maintenance or Failure:** A gateway requires maintenance due to:
 - Security vulnerabilities
 - Lack of periodic firmware updates
 - Inadequate authentication and authorization

- Degraded performance due to network instabilities
- Hardware or software failures
- Scalability and compatibility issues
- Insufficient processing power or memory

In this case, the connected assets are moved to an alternative gateway for uninterrupted connectivity and functionality.

- **Power Management:** In certain scenarios, it becomes necessary to move assets to gateways that are closer or have better power-saving features to conserve battery life and extend operational up-time.
- **Resource Optimization:** If a asset requires access to specific resources or services provided by a different gateway, it is moved to that gateway to use those capabilities effectively.

Note: Presently, INFER™ supports the moving of things that are direct (1st level) children of a gateway to being a direct children under another gateway, but **within the same organization**.

1. To access Asset Migration, on the INFER™ UI, go to **Inventory > Monitored Assets**. The **Inventory - Monitored Assets** page appears.
2. Click the checkbox against the desired asset in the list.
3. Go to **Actions > Asset Migration**. The **Asset Migration** pop-up appears.
4. Select the Thing and click **Next**.
5. Select the new Parent Asset that you want your Thing to be migrated with and click **Next**.
6. Review the changes and click **Migrate**.

11.6.1 Migration Prerequisites

To ensure the successful migration of things to other gateways, you need to meet all the criteria listed below:

1. **Maintenance State:** Verify whether if the things and their connected things are presently in maintenance. For more information, see [Asset Maintenance](#).
2. **Agent Version:** Verify whether both the old parent gateway and the new parent gateway have agents with versions equal to or greater than . For more information on updating Agent, see [Updating INFER™ Agent](#).
3. **Organization Alignment:** Verify whether the assets and their connected assets belong to the same organization.
4. **Single Gateway:** Verify whether the assets and their connected assets belong to a single root gateway.
5. **Gateway Hierarchy:** Only assets that are immediate children of a gateway can be moved.
6. **New Parent Gateway Template:** Verify whether the new parent gateway's template has the migrating asset's template assigned as a child template.
7. **No Active Campaigns:** Verify that there are no active campaigns running on the things and their connected things.

Note: Even if the campaign's status is **STOPPED** and if the campaign's state is not **COMPLETED**, the migration is not considered successful.

8. **No Pending Commands:** Ensure that there are no pending commands for the things and their connected things.

9. **No Pending Tasks:** Ensure that there are no pending tasks for the assets and their connected things.

11.6.2 Migrating Things & Gateways

To migrate a thing to another gateway, perform the following steps:

1. Under **Inventory > Monitored Assets**, select the check boxes of things that need to be migrated.

Note:

- Make sure that the **Enrollment State** of the things' you have selected for migration are in **MAINTENANCE** state. For more information on putting asset into MAINTENANCE state, see [Asset Maintenance](#).
 - Presently, INFER™ supports only migration of assets that are things (not gateways).
 - Selected assets needs to have same parent gateway for migration.
2. Go to **Actions > Asset Migration**. The **Asset Migration** pop-up appears as shown below:

Asset Migration

1 Select Assets

2 New Parent Asset

3 Review

Select Assets

Only the assets that are thing and in Maintenance state can be migrated to another asset.

1. Only things in maintenance state can be selected for migration.
2. Selected assets must belong to same parent gateway.

<input type="checkbox"/>	Name	Asset Type	Enrollment State	Parent Gateway Name
<input checked="" type="checkbox"/>	Pinnacle-Asset-BH01	GATEWAY	REGISTERED	

CANCEL NEXT

3. In the previous step, in case you selected a asset which was not in the **MAINTENANCE** state, click the highlighted icon as shown above to put the asset into the maintenance state.
4. Click **NEXT**.
5. Under **Parent Asset**, select the desired new parent asset from the drop-down menu, and click **NEXT**.
6. Under **Review**, review the information and click **SAVE**. You have successfully migrated the selected assets to a new parent asset.
7. However, if the agent running in the parent asset is not up-to-date, the migration has failed.

11.7 Unenrolling Assets

Prerequisite: To unenroll a gateway and its connected assets that are enrolled to the INFER™ Server, ensure the following:

1. The asset must be enrolled to the INFER™ Server.
2. The Gateway cannot communicate with the Server after it is unenrolled. The data of the unenrolled asset will still remain in the INFER™ Server. To delete the data, delete the asset.

Perform the following steps:

1. On the INFER™ UI, navigate to **Inventory > Monitored Assets**. The **Inventory - Monitored Assets** page appears.
2. Click the gateway or thing asset that you want to unenroll.
3. Click the **Actions** drop-down menu and select **Unenroll**.
4. Confirm your action by clicking **UNENROLL**.

You have successfully unenrolled a asset.

Note: This operation also unenrolls the connected assets.

11.8 Deleting Single or Multiple Assets

After unenrolling a asset, delete it so that the asset no longer appears in the list of assets.

Prerequisite: You must have the DELETE_DEVICE permission to perform this operation.

This action deletes the asset data from the INFER™ Server. You cannot retrieve the deleted data.

1. On the INFER™ UI, navigate to **Inventory > Monitored Assets**. The **Inventory - Monitored Assets** page appears.
2. Select the asset and click the delete icon on the top-right side of the screen to delete.
3. In the confirmation dialog box, verify that you are deleting the correct asset and click **DELETE**. You have successfully deleted a asset.

11.9 Viewing List of Files

You can view a list of files uploaded by the assets in INFER™ Console.

Prerequisite: Ensure that your asset is in **ENROLLED** state.

1. On the INFER™ UI, navigate to ******Inventory** > Monitored Assets****.
2. Click the asset name for which you want to search a file associated with it.
3. From the ... (3 dots) drop-down menu, click **Files**.
4. To search a file, enter the name of the file.
A list of files with the time stamp, size, modified date, and a download menu item are displayed.
5. Select a file and click **Download**.
The file is downloaded to your local repository.

11.10 Viewing List of Assets by Property

You can view the list of assets based on their property name and value.

Prerequisite: You must be a **Device Administrator** to perform this operation.

1. On the INFER™ UI, navigate to **Inventory > Monitored Assets**.
2. From the **Properties** drop-down menu, select **Search Property Name** and enter the *search value*.

3. Click **OK** and **APPLY**.

The list of assets with the selected property appears.

Note:

- The property keys listed in the drop-down menu is what is defined in the templates. Additional keys defined in the assets (not part of template) are not listed in the drop-down menu.
- The list of possible values for a given property key is from the actual asset values for a given property key.

11.11 Updating Bulk Custom Properties on Multiple Assets

With INFER™, you can add, delete, and update custom properties in bulk on multiple assets.

Prerequisite: You must be a **Device Administrator** to perform this operation.

Note: The custom property that you update on an asset does not impact the set of properties in the asset template. To use the newly added keys in Advanced Search, you must edit the asset template and add the keys.

Perform the following steps:

1. On the INFER™ UI, navigate to **Inventory > Monitored Assets**

The **Inventory - Monitored Assets** page lists the registered, enrolled, and unenrolled Gateway and Thing assets.

2. Select the checkboxes against the assets for which you want to update the custom properties.

Note:

- Assets can be from multiple templates.
 - Asset state can be Enrolled and Registered.
 - Asset Type can be GATEWAY and THING
3. Go to **Actions** drop-down menu > **Edit Custom Property**. The **Edit Custom Properties** pop-up appears as follows:

Edit Custom Properties

2 assets selected

Edit

Enter Key(s) and Value(s) to Update custom properties for the selected assets

Name	Value
+ Add	

New

Enter Key(s) and Value(s) to Create custom properties for the selected assets

Name	Value
+ Add	

Delete

Enter Key(s) to delete from the selected assets

Name
+ Add

CANCEL

SAVE

- Under **Edit**, click **+ Add** and enter keys and value to update custom properties for the selected assets.
 - Under **New**, click **+ Add** and enter keys and value to create custom properties for the selected assets.
 - Under **Delete**, click **+ Add** and enter keys to delete for the selected assets.
 - Click **SAVE**. You have successfully updated custom properties in bulk on multiple assets.
 - To verify if the values are added, click the asset name and **Properties**.
 - Click **Custom Properties**. You can see that the properties are added.
 - To verify if the keys are deleted, click the assets name and **Properties > Custom Properties**. The keys have been deleted from the **Custom Properties** for the assets.
- Note:** You can ADD, EDIT, or DELETE any custom property using the bulk command.

11.12 Editing Custom Properties via Spreadsheet

You can edit custom properties of assets in bulk using .xlsx from the INFER™ Console.

- On the INFER™ UI, navigate to **Inventory > Monitored Assets**.

The **Inventory - Monitored Assets** page lists the registered, enrolled, and unenrolled Gateway and Thing assets.

- Click the check boxes against your desired set of assets.
- Next, at the top right, click **ACTIONS > Edit Custom Properties via Spreadsheet**. The following pop-up appears:

Edit Custom Properties via Spreadsheet ×

Total 1 Asset(s) selected, Editing the Custom Properties of the asset(s) using a Spreadsheet file is done in three steps

Step 1 - Download the Spreadsheet contains Custom Properties of the Asset(s)

DOWNLOAD SPREADSHEET

Step 2 - Edit the Spreadsheet

In the downloaded Spreadsheet,

- Do not Delete/Edit the existing Sheet
- Do not Delete/Edit the existing Column headers
- Please do not edit following Column's cell:

Asset Id Asset Name Asset Type Asset State Template Name
- New custom property could be added by adding the column header
- Existing Asset's Custom Properties that match by ID will be updated
- Rows that do not consist the ID will be skipped
- The Custom property would be removed if it's value is empty
- File format should be in .xlsx format

Step 3 - Upload the Updated Spreadsheet

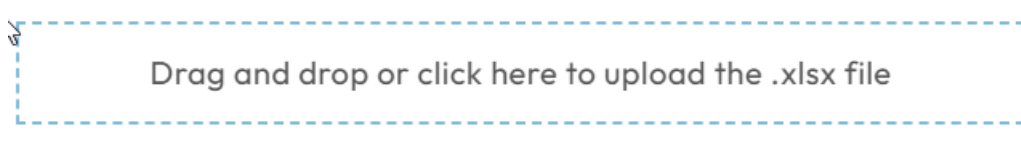
CANCEL UPDATE

- Click the check box if you want to select all the listed assets across all pages.
- Click **DOWNLOAD Spreadsheet**.
- Edit the `.xlsx` file by following the rules listed below:

Note:

- Do not remove/edit the existing Column headers
- Do not edit following Columns' cells:
 - Asset Id
 - Asset Name
 - Asset Type
 - Asset State
 - Template Name

3. Add new custom property by adding new column header.
4. Existing Assets' Custom Properties that match by ID will be updated.
5. Rows that do not have the ID will be skipped.
6. A custom property will be removed if it's value is left empty.
7. File format should be saved in *xlsx* format only.
7. Drag and drop the filled Spreadsheet in to the marked area or click the area as shown below:



8. Click **UPDATE**. You have successfully updated the assets' custom properties.

11.13 Collecting Metrics using DefaultClient Binary

After you install the INFER™ Agent, a daemon process starts and the DefaultClient binary sends the default metrics such as CPU usage, memory usage, and disk usage to the INFER™ Agent every 60 seconds.

The Agent collects the metrics and sends them to the INFER™ Server based on the metric interval time set in the asset template. The default metric interval time is 60 seconds.

While creating a asset template, ensure that you do not remove the **CPU-Usage**, **Memory-Usage**, and **Disk-Usage** metrics that are available in the template by default to monitor the performance of a gateway.

Note: Ensure that you do not change the metrics name and data type.

The DefaultClient binary is available in the gateway at

```
/opt/smarthub/iotc-agent/bin/
```

To run the binary with any other custom-defined metric in the asset template, run the following command:

```
/opt/smarthub/iotc-agent/bin/DefaultClient send-metric --
device-id=<device Id> --name=<metric name> --
type=<string|integer|double|boolean> --value=<value>
```

11.14 Viewing Metric Graphs

The metric graph data is aggregated if there are more than 1000 numeric metric values in a selected range. Each aggregated data point is an average of the values for a given time period within the range.

Note: String and Boolean values are not aggregated and are limited to the latest 1000 data points. To view all the data values, select a smaller time range.

To view the graph of the metrics collected on your asset, perform the following steps:

1. On the INFER™ UI, navigate to **Inventory > Monitored Assets**.

The **Inventory - Monitored Assets** page lists the registered, enrolled, and unenrolled Gateway and Thing assets.

2. Click the asset for which you want to view the metrics graphs and click the **Metrics** tab.

By default, graphs are displayed for the following metrics:

- CPU-Usage (in %)

- Memory-Usage (in %)
- Disk-Usage (in %)

12 Working with Campaigns

This chapter explains campaigns, and lists steps to run campaigns to update and track the software, firmware, operating system, and BIOS of your gateway device using's **Campaigns** sub-module.

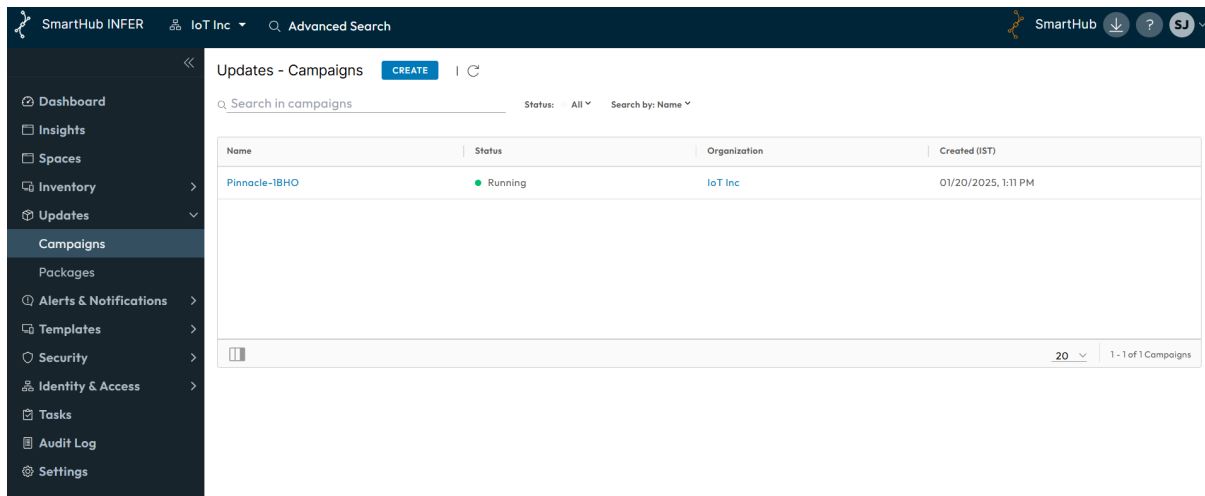
12.1 What is a Campaign?

A campaign in INFER™ is a coordinated series of planned actions performed by you that distributes specific OTA update packages to specific devices along with details of the update process and its associated controls.

A campaign delivers packages to the Agent which in turn deploys multiple enrolled target devices in INFER™. A campaign also monitors the device's update status and displays alerts in case of failed updates.

In the **Campaigns** sub-module, you can:

- Create a campaign
- Clone a campaign
- Edit a campaign
- Delete a campaign
- Stop a campaign
- Add a distribution select query to the campaign
- Associate update packages to the devices in your campaign



12.1.1 Distribution Select Query

Distribution queries are search filter definitions whose results are the listed devices on which the campaign runs. A Distribution Select Query periodically matches a subset of all the registered devices that fulfill the query.

Using the **Campaigns** sub-module, you can specify an existing Distribution Select Query or create a new query to run a campaign.

To add specific devices to the campaign, call the **addTargetGateways** API.

For more information about Campaign Management APIs, see the [INFER™ API Reference Guide](#).

12.1.2 Using Advanced Search

Advanced Search allows you to search for devices based on multiple search parameters.

Advanced Search

New Search SAVE AS

Asset Template

GATEWAY

Key

id

Operator

Contains

Value

70abd3e3-f96c-448f-9e50-a5003a6c29ce

Enter value

Columns

name x deviceType x Location x enrollmentState x

SEARCH

CLEAR

+ ADD KEY

EXPORT AS CSV

Asset ID	Organization	enrollmentState	name	deviceType	Location
70abd3e3-f96c-448f-9e50-a5003a6c29ce	AN-Test	ENROLLED	AN-Test-June21	GATEWAY	

Finished 1 - 1 of 1 Assets

Advanced Search finds only those devices that meet all your search criteria. You can select multiple values for a key condition, and the search finds the device whose key meets any of the values.

You can search for devices using the following parameters:

- **Asset Template:** You can search with templates designed for asset.
- **Key:** You can search with campaign name campaign state, metric names, asset type and so on. If your keys include a metric name, you must set a time range for that metric condition. You can also enable the **Relative Timestamp** option to select a time range starting from the current date and time.
- **Operator:** Use the operators to select values for each key.
- **Columns:** Select the columns that you want the search results to display, such as **Campaign Name**, **Campaign State**, **Asset Type**, **Location**, and so on. **Asset Id** always appears as the first column. For example, you can search for all Dell Edge 3000 gateways that exceeded 90% of the CPU utilization in the last 24 hours.

12.1.2.1 Saving a Filter Definition You can save your filter criteria as a filter definition. When performing an over-the-air campaign, you can use that saved filter definition to select the devices for the distribution list.

Note:

- Ensure that the filter definition name is 35 characters or less in length.
- You cannot delete or modify the search criteria of a distribution list if they are associated with a campaign. You must delete the campaign first.

To perform advanced search operations, click **Advanced Search** on the top menu bar of the Console.

12.1.2.2 Exporting Search Results To export a search result in the **CSV** format, perform the following steps:

1. From the **Advanced Search** results page, click **EXPORT AS CSV** as highlighted in the previous section.
2. The search results are downloaded a **CSV** file (`search-results_2024-05-27_141407.csv`).

12.2 Campaign Approvals

By default, a campaign does not require an approval when you create it unless you configure your organization's settings to check for campaign approvals. Furthermore, the Campaign Administrator's role has permissions to approve campaigns.

If necessary, a System Administrator can create a role with campaign approval permissions and remove the campaign approval permissions from the Campaign Administrator's role.

If your campaigns (OTA) require an approval before starting, toggle the **Enable Approval** option under the **Settings>Updates** tab.

- Users with permissions to edit organization settings can set the approvals for campaigns.
- Users with campaign approval permissions can approve a campaign.

Note: Approval settings for existing campaigns will not change after updating your organization settings.

12.2.1 Campaign Approval Use Cases

Prerequisites: To perform the campaign operations in INFER™, you must have the following Campaign permissions associated with the Organization Administrator Group.

- CREATE_PACKAGE
- EDIT_PACKAGE
- DELETE_PACKAGE
- VIEW_PACKAGE

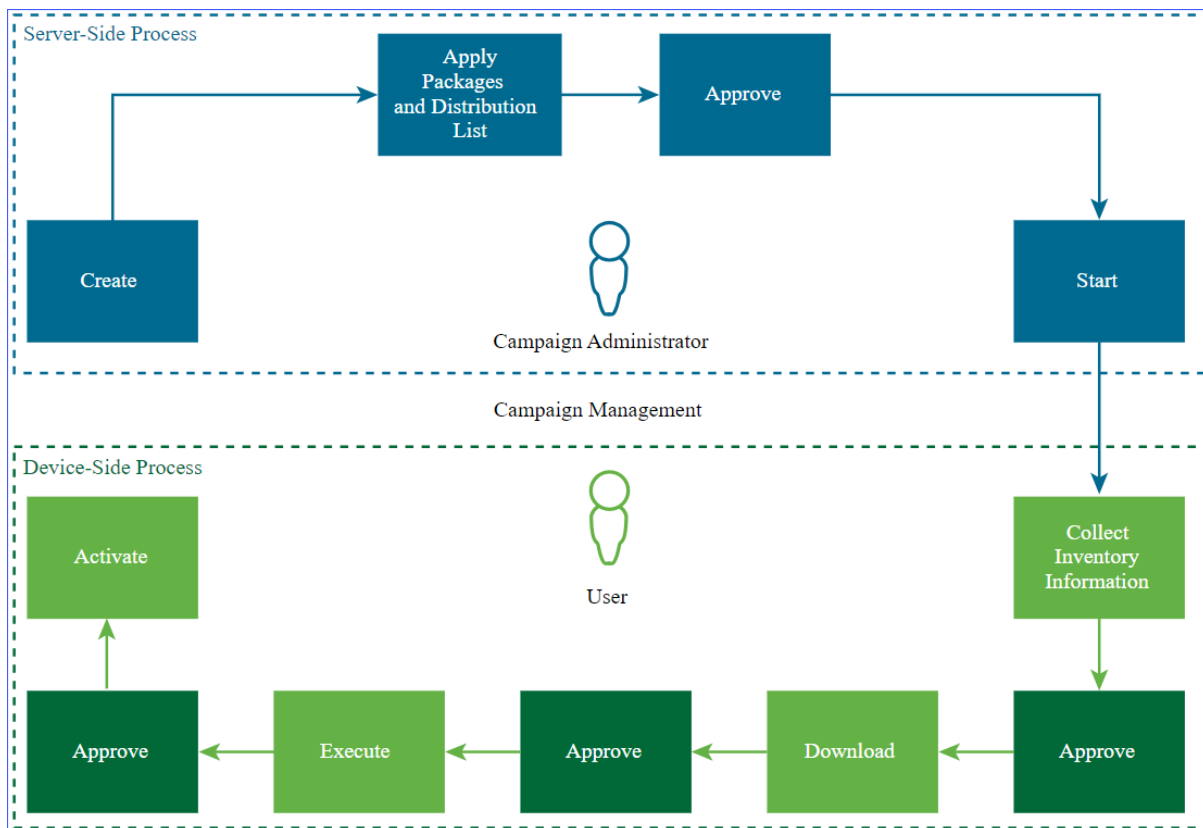
The following use cases describe the campaign approval process:

1. Your organization does not require approvals for campaigns. You need not make any changes.
2. Your organization requires approvals for campaigns. A user with the Campaign Administrator role must approve the campaigns:
 - a. The System Administrator creates a user with the role to edit organization settings.
 - b. The user edits the Approve Campaign settings.
 - c. A user with the Campaign Administrator role approves the campaign.
3. Your organization requires approval for campaigns from a special role that has the Approve Campaign permission.
 - a. The System Administrator creates a special role with Approve Campaign permission. The user who approves campaigns must also have the following permissions:
 1. View Campaign
 2. View Package
 3. View Organization Settings
 4. View Package
 5. View Filter Definition
 6. Edit Filter Definition
4. The System Administrator removes the Approve Campaign permission from the Campaign Administrator role.

5. The System Administrator creates a user and assigns the special role that has the Approve Campaign permission.
6. The System Administrator creates a user with the Edit Organization Settings role. This user edits the Approve Campaign settings.
7. The user with the Campaign Administrator role creates campaigns.
8. The user with the special role approves the campaigns.

12.3 Campaign State Transition Scheme

The following diagram illustrates the different states of a campaign.



Note: For a headless campaign execution, approvals for downloading, executing, and activating packages are not required.

12.4 Creating a Campaign

To create a campaign, perform the following steps:

1. Create an IoT Package. For information about creating an IoT Package, see **Building a Package**.
2. On the UI, navigate to **Updates > Campaigns**. The **Updates - Campaigns** page appears.
3. Click **CREATE**. The **Create Campaign** wizard appears as shown below:

The screenshot shows the 'Create campaign' interface. On the left is a sidebar with five steps: 1 Details (selected), 2 Distribution Select Query, 3 Select Package, 4 Start Options, and 5 Review. The main content area is titled 'Details'. It contains a 'Name' field with a red asterisk and a placeholder 'Enter Campaign Name'. Below it is a 'Description' field with a placeholder 'Enter Campaign Description'. At the bottom right of the form are two buttons: 'CANCEL' and 'NEXT'.

4. Under **Details**, enter a name and under Description, enter a brief description for your campaign.
5. Click **NEXT**.
6. Under **Distribution Select Query** you can select devices based on the search conditions set. For more information, see [Distribution Select Query](#).
 1. To run the campaign on all registered gateways, select **All registered gateways**.
 2. From the **Update asset template type** drop-down menu, select **GATEWAY** or **THING** to run the campaign on a gateway or a Thing device.

Note: If you select **THING**, add the **parentGatewayId** property in the columns when creating the distribution query.
 3. From **Distribution Select Query** drop-down menu, select the desired option. Alternately, click **+ Create New** icon to create a new distribution query:
 1. From the **Asset Template** drop-down menu, select the type of asset template to filter.
 2. From the **Key** drop-down menu, select the desired metric that you want to filter the assets by. Click **+ Add Key** to create a new key.
 3. Next, from the **Operator** drop-down menu, select the desired operator.
 4. In the **Value** text box, enter the metric values.
 5. Enter a name for the distribution list and click **SAVE AS**. You have successfully saved the query as a new **Advanced Search** query. You can also select this query next time you want to create a campaign that requires similar assets to be included.
 4. Click **NEXT**.
7. Under **Select Package**, select the update packages you want to associate your campaign with. You can select multiple packages of the same type. Click **Next**.

Note: You can edit packages and distribution lists for the campaigns that are created, but you cannot edit them for those campaigns that are in the **Approved** or **Started** state. To edit these packages and distribution lists, you must delete the campaign first.
8. Under **Start Options**, click the desired option and click **NEXT**.
9. Under **Review**, review your campaign information and click **CREATE**. You have successfully created a campaign.

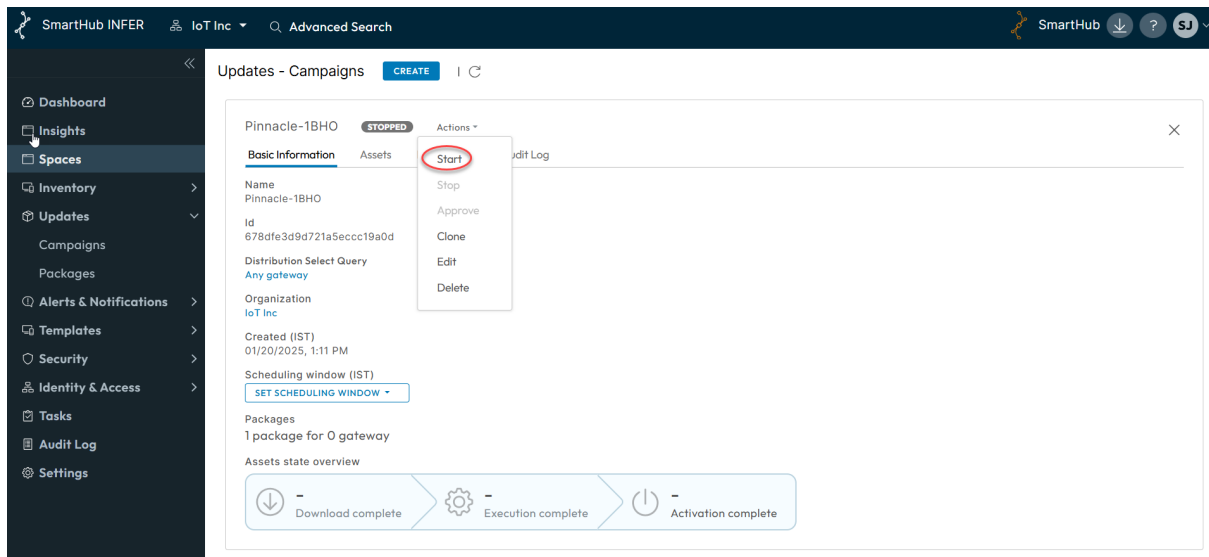
12.5 Starting a Campaign

Prerequisites: Before you run the campaign you have created, keep the following conditions in mind:

1. The campaign adds and processes only the gateways or Thing devices that are in the ENROLLED state.
2. You must have created a campaign and it must be in the APPROVED state.
3. You cannot start a scheduled campaign manually.
4. The campaign adds and processes only the gateways or Thing devices that are in the ENROLLED state.
5. You must have created a campaign and it must be in the Approved state.
6. You cannot start a scheduled campaign manually.

To start the campaign you have created, perform the following steps:

1. On the UI, navigate to **Updates > Campaigns**. The Campaigns page appears.
2. From the listed campaigns, click the campaign you desire to run.
3. Under **Actions**, click **Start** as highlighted below.



The campaign runs on all the enrolled Thing devices on a gateway whose **parentGatewayId** is listed in the distribution search query. The campaign is processed as a whole on all the devices that match the search criteria and are connected to one gateway, and they transition through the campaign states together.

When you enroll a new Thing device to your gateway and if it matches the campaign distribution query, the campaign restarts on all the connected Thing devices irrespective of their states. To view the state of your campaign, click the **Asset** tab.

Note:

1. Once you start a campaign, the distribution list is evaluated and the resulting devices are added to the campaign.
2. It takes 30 minutes for the newly enrolled devices that match the distribution list's criteria to be added to the campaign.
3. You cannot edit the filter definition list after the campaign starts. You cannot start a scheduled campaign manually.

12.6 Cloning a Campaign

Cloning a campaign offers several advantages, particularly when you are running multiple campaigns that share common elements or configurations. Listed below are some advantages of cloning a campaign:

- **Efficiency:** Cloning a campaign saves time and effort by allowing you to replicate the structure and settings of a successful campaign. You need not recreate everything from scratch.
- **Consistency:** Ensures consistency across campaigns by using a standardized configuration.
- **Reduces Errors:** Since you're working with a proven campaign, there's a lower chance of making configuration errors that could disrupt your OTA campaign.
- **Faster Deployment:** Speeds up the deployment of new campaigns since much of the initial setup work is already done in the template.
- **Cost Savings:** Saves money by reducing the need for extensive customization and development work for each new campaign.
- **Scalability:** Facilitates the scaling of campaigns. You can easily create multiple instances of the same campaign to manage larger deployments.
- **Ease of Management:** Simplifies campaign management by providing a consistent interface for monitoring and control.
- **A/B Testing:** Makes A/B testing easier because you can create variations of a campaign to test different strategies and compare their performance.
- **Version Control:** Provides a clear starting point for version control. You can track changes made to the template and maintain a history of campaign configurations.
- **Rapid Prototyping:** Speeds up the process of prototyping new IoT campaigns or concepts by starting with a known template and making adjustments as needed.
- **Adaptability:** Allows you to adapt and modify a campaign to suit the specific requirements of each campaign while retaining the core structure.
- **Security:** Ensures that security configurations and best practices are consistently applied across campaigns.

To clone a campaign, perform the following steps:

1. On the UI, navigate to **Updates > Campaigns**. The **Updates - Campaigns** page appears.
2. From the listed campaigns, click the campaign you desire to clone.
3. Next, under **Actions**, click **Clone**. The **Create campaign** wizard appears.
4. Under **Name**, enter the new campaign name.

Note: Else, the existing campaign name will be appended as `Xxxxxxxx_clone`.

1. Under **Description**, enter a brief description of the new campaign and click **NEXT**.
2. Under **Distribution Select Query** you can select devices based on the search conditions set.
 1. To run the campaign on all registered gateways, select **All registered gateways**.
 2. From the **Update asset template type:** drop-down, select **GATEWAY** or **THING** to run the campaign on a gateway or a Thing device.

Note: If you select **THING**, add the `parentGatewayId` property in the columns when creating the distribution query.

3. From **Distribution Select Query** drop-down menu, select the desired option. Distribution queries are search filter definitions whose results are the assets on which the campaign runs.

Alternately, click **+ Create New** to create a new distribution query:

- a. From the **Asset Template** drop-down menu, select the type of asset template to filter.
 - b. From the **Key** drop-down menu, select the required metric that you want to filter the devices by. Click **+ Add Key** to create a new key.
 - c. Next, from the **Operator** drop-down menu, select the desired operator.
 - d. In the **Value** text box, enter the metric values.
 - e. Enter a name for the distribution list and click **SAVE AS**. You have successfully saved the query as a new **Advanced Search** query.
You can also select this query next time you want to create a campaign that requires similar devices to be included.
4. Click **NEXT**.
 3. Under **Select Package**, select the update packages you want to associate your campaign with. You can select multiple packages of the same type. Click **Next**.
Note: You can edit packages and distribution lists for the campaigns that are created, but you cannot edit them for those campaigns that are in the **Approved** or **Started** state. To edit these packages and distribution lists, you must delete the campaign first.
 4. Under **Start Options**, click the desired option and click **NEXT**.
 5. Under **Review**, review your campaign information and click **CREATE**.
You have successfully created a campaign.

12.7 Editing a Campaign

Before you edit a campaign, keep the following conditions in mind:

1. You can edit only those campaigns that are in the **CREATED** state.
2. When a campaign transitions from the **STOPPED** state to the **STARTED** state, you can modify only its name.
3. You can edit an approved campaign when the system does not require approvals. You cannot edit the distribution query.

To edit an existing campaign in **INFER™**, perform the following steps:

1. On the UI, navigate to **Updates > Campaigns**. The Campaigns page appears.
2. From the listed campaigns, click the campaign you desire to edit.
3. Under **Actions**, click **Edit**. The **Edit - Campaign** pop-up appears. Here, update the **Name** and **Description** and click **NEXT**.
4. Under **Review**, review the information and click **SAVE**. You have successfully edited a campaign.

12.8 Deleting a Campaign

Before you delete a campaign, keep the following condition in mind:

- You can only delete those campaigns that are in the **created** or in the **ended** states.

To delete an existing campaign in **INFER™**, perform the following steps:

1. On the UI, navigate to **Updates > Campaigns**. The Campaigns page appears.

2. From the listed campaigns, click the campaign you desire to edit.
3. Under **Actions**, click **Delete**. The **Delete Campaign** pop-up appears as shown below:

Delete Campaign

Are you sure you want to delete the campaign? The operation will fail if there is an ongoing device update.

☐ Ignore ongoing updates and delete anyways

CANCEL
DELETE

4. Click the checkbox if you want to **Ignore ongoing updates and delete anyways**.
5. Click **DELETE**. You have successfully deleted a campaign.

Note: You can stop a campaign only if the asset in the campaign are in a state before the **DOWNLOAD** state.

For more information about Campaign Management APIs, see **Running a Campaign Using Agent SDK** chapter in the see the [INFER™ API Reference Guide](#).

12.9 Controlling Campaigns using DefaultClient CLI

This chapter details the prerequisites and steps to run over-the-air (OTA) updates on a Gateway, using the **DefaultClient** CLI.

Campaign services use the following properties from the IoTCAgent:

- `commandFetchIntervalSeconds` : The IoTCAgent makes periodic `get-command` requests to the micro services for every `commandFetchIntervalSeconds` expiry.
- You can configure the property value through the **Asset Template** tab in the Console.

By default, the IoTCAgent runs with the following property values:

```
commandFetchIntervalSeconds=30 manifestExecution=ENABLE
```

When you start the IoTCAgent with the default properties, it requests for command instructions from the Server by calling the `get-command` every 30 seconds.

Note: For each lifecycle phase, the IoTCAgent receives a command from the Server to perform the download, execute, and activate operations.

12.9.1 Running a Campaign using Default Properties

You can run an OTA update for the IoTCAgent using default properties by performing the following steps:

1. Using the [Creating a Package using Package Builder](#) or the [Using Package Management CLI to Register Multiple Assets](#) tool:
 - a. Create an IoT Package. For more information about creating the IoT Package, see [Creating a Package using Package Builder](#).

- b. Upload the IoT Package to the repository. Alternately, you can use the Console to upload to the repository. For more information about uploading the IoT Package, see [Uploading the IoT Package](#).
2. Enroll asset.
3. Create a campaign using a distribution select query and the packages that you uploaded while creating the campaign.
4. Start the campaign.

The IoTCAgent auto-polls the command instructions every 30 seconds. The campaign states flow from **INITIALIZED** to **COMPLETED** after a series of get-commands calls to the Campaign Server.

12.9.2 Running a Campaign in On-Demand Mode

Perform the following steps to run an OTA update for the IoT Agent in the On-Demand mode, that is, with the `commandFetchIntervalSeconds` property set to `0`. This property value is defined in the device template.

1. In the specification file, set the value of the `headlessExecution` execution property to `false`.
2. Using the [Creating a Package using Package Builder](#) or the **Package Management CLI for Advanced Users** tool, perform the following steps:
 - a. Create an IoT Package.
 - b. Upload the IoT Package to the repository. Alternately, use the Console to upload to the repository.
3. Create a campaign using a distribution select query and the packages that you uploaded while creating the campaign.
4. Start the campaign.

The IoTCAgent invokes the `get-commands` when initiated from the `DefaultClient` binary. The following example outlines the different states of the Gateway during an OTA update. The state of the Gateway is **INSTANTIATED** when the OTA campaign starts.

12.9.3 Sample Workflow

1. Invoke the get-commands to call from the `DefaultClient` or an Agent SDK extension. The state of the Gateway changes to **INVENTORY_UP_TO_DATE**.
2. Invoke the get-commands to call from the `DefaultClient` or an Agent SDK extension. The state of the Gateway changes to **WAITING_FOR_*_APPROVAL**.

In the **WAITING_FOR_*_APPROVAL** state, schedule the next state. For example:

```
DefaultClient schedule --type=download --campaignid=<campaign id>
DefaultClient schedule --type=download --campaignid=<campaign id>
↪ --start-time=0 --end-time=0
DefaultClient schedule --type=download --campaignid=<campaign id>
↪ --start-time=5000 --end-time=80000
```

Based on the campaign scheduled time, the state of the device changes from **SCHEDULED_DOWNLOAD** to **WAITING_FOR_DOWNLOAD**.

3. Invoke the get-commands to call from the `DefaultClient` or an Agent SDK extension. The Gateway starts downloading the package and the state of the device changes from **DOWNLOADING** to **DOWNLOAD_COMPLETE**.

4. Invoke the get-commands to call from the `DefaultClient` or the Agent SDK extension. The state of the Gateway changes to `WAITING_FOR_EXECUTION_APPROVAL`.

Here, you can schedule a start and end time for running the campaign using the following command:

```
DefaultClient schedule --type=<download|execution|activation>
↪ --campaignid=<campaign Id> [--start-time=<start time window>
↪ --endtime=<end time window>]
```

For example:

```
DefaultClient schedule --type=execution --campaignid=<campaign id>
DefaultClient schedule --type=execution --campaignid=<campaign id>
↪ --start-time=0 --end-time=0
DefaultClient schedule --type=execution --campaignid=<campaign id>
↪ --start-time=5000 --end-time=80000
```

Based on the campaign scheduled time, the state of the device changes from `SCHEDULED_EXECUTION` to `WAITING_TO_EXECUTE`.

Here, you can schedule a start and end time for activating the campaign using the following command:

```
DefaultClient schedule --type=<download|execution|activation>
↪ --campaignid=<campaign Id> [--start-time=<start time window>
↪ --endtime=<end time window>]
```

For example:

```
DefaultClient schedule --type=activation --campaignid=<campaign id>
DefaultClient schedule --type=activation --campaignid=<campaign id>
↪ --start-time=0 --end-time=0
DefaultClient schedule --type=activation --campaignid=<campaign id>
↪ --start-time=5000 --end-time=80000
```

Based on the campaign scheduled time, the state of the device changes from `SCHEDULED_ACTIVATION` to `WAITING_TO_ACTIVATE`.

Note: Contact your Device Administrator or Campaign Administrator if the state of the Gateway changes to one of the following states:

- `DOWNLOAD_FAILED`
- `EXECUTION_FAILED`
- `ACTIVATION_FAILED`

12.9.4 Running a Campaign in Headless Mode

This section lists the prerequisites for running a campaign for the IoT Agent in Headless Mode.

- Run the IoTAgent with the `manifestExecution` property set to `ENABLE`: `manifestExecution=ENABLE`

On any campaign, the `get-commands` call ensures that the OTA updates are auto-delivered to the IoTAgent. The `get-commands` calls from the IoT Agent listens to the Campaign commands and the campaign downloads, executes, and activates updates.

12.9.5 Monitoring Campaign Progress

To monitor the progress of a campaign on the gateway, set the `agentLogLevel` to `6` in the `iotc-agent.cfg` file. You can then monitor the system logs to view the progress of the campaign using tools such as `journalctl -u` or `iotc-agent -f`.

12.9.6 Approving OTA Update Phases

Depending on the IoTCAgent configuration and the package property for headless execution, there are check points in the device or gateway that may require an approval for the campaign to run.

- You can configure your OEM or SI application to use these checkpoints to schedule a maintenance window for updates, or for approving the campaign to run the updates.
- You can monitor the device or gateway's campaign progress from the **Campaigns** tab in console. To view the progress of the campaign, select the campaign from the list and click the **Assets** tab.

Note: The default interval for the IoTCAgent to fetch new commands from the Server is 30 seconds. You can change the interval value through the Asset Templates settings in the INFER™ Console.

Use the following commands to configure the campaign execution settings using the **IoTCAgent SDK** or the **IoTCAgent CLI**:

- After the campaign reaches the **Waiting for Download Approval** state:

```
DefaultClient schedule \--type=download \--campaign-id=<campaignId>
```

Note: Copy the campaign ID from the Campaigns page of the Console.

- After the campaign reaches the **Waiting For Execution Approval** state:

```
DefaultClient schedule \--type=execution \--campaign-id=<campaignId>
```

- After the campaign reaches the **Waiting For Activation Approval** state:

```
DefaultClient schedule \--type=activation \--campaign-id=<campaignId>
```


13 Working with Package Builder

This chapter explains the update package, and lists steps to upload and build update packages, using's **Packages** sub-module.

13.1 What is a Package?

A package is an update unit containing all actions required for managing a device over the air (OTA).

Using packages, you can:

- Update the operating system of a gateway device
- Install or update an application
- Reconfigure the gateway settings
- Update the devices' BIOS and firmware
- Run campaigns using Package Builder

13.2 Creating a Package using Package Builder

Prerequisite: To build update packages in INFER™, you must have the following Campaign permissions associated with the Organization Administrator Group.

- CREATE_PACKAGE
- EDIT_PACKAGE
- DELETE_PACKAGE
- VIEW_PACKAGE

Note: If you are an Advanced user, you can create a package file using the **Package Management CLI** tool.

1. On the INFER™ UI, navigate to **Updates > Packages**. The **Updates - Packages** page appears as shown below:
2. Click **BUILDER**. The **Package Builder** wizard appears as shown below:

Package Builder

- 1 Details
- 2 Attachments
- 3 Manifest
- 4 Review

Details

Name *

Name

Version *

Version

Operating system * **Architecture ***

Select OS Select Architecture

Description

Description

Labels

CANCEL **NEXT**

- Under **Name**, enter the package's name.
- Under **Version**, enter the package's version number.
- Under **Operating system**, select the required OS from the drop-down menu.
- Next, under **Architecture**, select the required architecture from the drop-down menu.
- Under **Description**, enter a brief description of the package.
- Under **Labels**, enter package-specific keywords to help future search.
- Click **NEXT**.
- Under **Attachments**, click **+ Add** and browse your local folder and select package files with `.sh`, `.py`, `.json`, `.ini`, `.service`, `.txt`, `.bin` extensions.
- Click **NEXT**.
- Under **Manifest > Headless Execution** appears switched ON by default. This controls the automatic transition of each lifecycle phase without any interaction.
- Under **Lifecycle** from the drop-down, select and add the package's desired lifecycle phase.

Note: Here, you can define the different lifecycle phases and the corresponding 'action' - an executable file (must match from **Attachments** section) or binary command with arguments that performs the required tasks for the current phase.
- Next, click the **Edit** icon and under **Action** select files attached by you in the previous step, as highlighted below:

15. Next, under **Arguments**, if needed, enter associated arguments for the above action.

Note:

1. When you add lifecycle phases, they are added in the following sequence:

1. **entrypoint**
2. **verify**
3. **execute**
4. **validate**
5. **activate**
6. **reset**

2. You can attach executables to all lifecycle phases except the entrypoint phase. The executable for the entrypoint phase must be present on the Gateway's file system and ready to run.

3. These lifecycle phases are optional.

If you use lifecycle phases, you cannot modify the phases or the order in which the phase actions are run. If you do not specify executables in the **action** field, then no action is performed and the phase is considered to pass successfully and the lifecycle moves to the next phase.

For example, if you do not provide a *verify.sh* executable in the **verify** phase, the package runs without verification (other than the default verification steps provided in the packaging format, such as checksum and RPM signatures), and moves to the **validate** state.

This process continues until the package moves to the **activate** phase. The phases **activate** and **reset** are mutually exclusive. The update is either activated or reset depending on the **validate** phase result.

Note:

- For all the executables that are attached for the action field, the IoT Agent sets the execute permission to `(700 / -rwx-----)` for the *iotc* user by default.

- If there are other executables listed in packages/files/scripts beside the executables that are specified in the action field, the author of the executables must manage the required permissions.

16. Click **DONE**.

17. Click **NEXT**.

18. Under **YAML Review**, review the package information you entered and click **SAVE**. You have successfully built and uploaded a new package update.

19. The newly created package appears.

After you complete the above steps, you can:

- Use the package to create the campaign.
- Download the package if required. To download a package, select the package and click the download icon on the right side of the page.
- On the Console, the file upload and download operations run in the background and the results appear after the operations are complete.
- You cannot overwrite packages or delete them when they are associated with a campaign that is approved or started at least once.

Note: From release 2019.09 onwards, you cannot upload packages to using the 2019.07 version of the **Package Management CLI** tool. Ensure that you download the latest version.

14 Package Management CLI for Advanced Users

A package is an update unit containing all actions required for managing a device over the air (OTA).

This chapter lists specific steps for advanced users to manually create a Specification (`YML`) file by using the **Package Management CLI** tool to build update packages.

The Specification (`YML`) file defines all actions and any other meta data to run a campaign.

Note: - The Package File in INFER™ is called IoT package.

- For creating and uploading packages, download the latest version of the Package Management CLI tool from INFER™.

14.1 Creating a Specification YML File

To create an `IoT package` , a specification file (`YML`) is required. The `YML` file describes the content of the package and its associated metadata. You must create a `YML` file before creating an *IoT package*. For more information, see [Using Package Management CLI to Register Multiple Assets](#) tool:

The `package-cli.zip` archive contains the `example-iotc-package` folder. Review the contents in this folder before creating the IoT package.

Alternately, you can use the following sample `YML` file as a template to create a file named `test_package.yml` . Change the values in the `test_package.yml` file according to your organization's requirements.

```
package:
  manifest:
    headlessExecution: true
    lifecycle:
      # Note the paths written in the action sections.
      If they don't match
        # any of the install paths in the attachments section, the tool will
        # warn you, but it will make a package. This is so you can address
        # executables that are on the GW but not in this package, but this
        # requires a full path to be specified in the action section.

        - phase: verify
          action: <parent directories of build
machine>/example-iotc-package/package-source/verify.sh
        - phase: execute
          action: <parent directories of build
machine>/example-iotc-package/package-source/execute.sh

        # This phase's action matches the install path of the validate.sh
        # attachment, so no warning will be issued.
        - phase: validate
          action: <parent directories of build
machine>/example-iotc-package/package-source/validate_package.sh

        # This phase's action points to an attachment that doesn't match
        # any install path, even though there is an attachment named activate.sh
        - phase: activate
          action: activate.sh
        - phase: reset
```

```

    action: <parent directories of gateway>/reset.sh
attachments:
  # path describes where the attachments are on the
  system you're building the package.
  # installPath describes where on the gateway the
  attachment will be installed.
  # If installPath is not added, the 'path' value will be used.
  # Any the directories in the installPaths that don't exist on the gateway
  # will be created.
  - path: <parent directories of build machine>/
    exampleiotc-package/package-source/test_file.txt
  - path: <parent directories of build machine>/
    exampleiotc-package/package-source/verify.sh
  - path: <parent directories of build machine>/
    exampleiotc-package/package-source/execute.sh
  - path: <parent directories of build machine>/
    exampleiotc-package/package-source/validate.sh
  # This will install the validate.sh attachment
  # in the same directories but named validate_
  package.sh
installPath: <parent directories of build
machine>/example-iotc-package/package-source/
validate_package.sh
  - path: <parent directories of build machine>/
    exampleiotc-package/package-source/activate.sh
  - path: <parent directories of build machine>/
    exampleiotc-package/package-source/reset.sh
  # You can specify a completely different directory
  # for attachment installation
installPath: <parent directories of
gateway>/reset.sh

name: hello_iotcp
# This is one of the many ways you can create a multiline string in yaml
description: "A test IoT Center package within a multiline description."
version: 1.1.0

# This tag is empty. That means the tool will default to noarch.

architecture:

  # This is a simple string, so you could write anything, however, there are
  # standardized names for various operating systems.
  # If this tag is empty, the tool will use the value which was
  # used to compile it for the respective OS (windows, linux
  or darwin).
  # If it is not able to read the compile-time value or it's empty, it will
  # default to noos.
os: linux
  # This is a simple array of strings which are just that -
  labels by
  # which you could search a package in INFER.
labels:
  - test
  - example

```

In this example:

The `attachments` section lists the files to be included in the package:

- `path` - The path on the disk where the file to be included in the package is located.
- `installPath` - The path on the gateway where the attachments are installed.

Note:

- If `installPath` is not specified, the `path` value is used.
- If any of the directories specified in the `installPath` do not exist, they are created on the gateway if the `iotc-user` has the required permissions.

The `manifest` section describes the package lifecycle and execution. It allows custom actions to be associated with lifecycle events.

The `headlessExecution` flag:

- Controls the automatic transition of each lifecycle phase, without any interaction. By default, the value is `true`.
- If `headlessExecution` is set to `true` and the IoT Agent is configured with `manifestExecution = ENABLED`, then the campaign runs automatically without any interaction.
- If `headlessExecution` is set to `false` and the IoT Agent is configured with `manifestExecution = ENABLED`, then the campaign scheduling depends on an external input runs automatically without any interaction.
- If `headlessExecution` is set to `false` and the IoT Agent is configured with `manifestExecution = ENABLED`, then the campaign scheduling depends on an external input such as `DefaultClient` or SDK client that must be registered with the IoT Agent. The executable specified for a particular phase is run by the IoT Agent at each lifecycle phase.
- If the IoT Agent is configured with `manifestExecution = DISABLED`, then the `headlessExecution` property and the executable steps are ignored. Here, all the associated executables are disabled and an SDK client must be configured to run the campaign.

`action` - An executable file that performs the required tasks for the current phase. For example, the executable file performs tasks such as verifying the downloaded content, setting up the environment, running the installer, and validating whether the installation is successful.

The executable file is run in an isolated shell that has the environmental variable `DATADIR` set to the path of the directory that contains the extracted package files. If relative paths are used, `DATADIR` is set to access the files. For example, the path to access the `update_data.tar.gz` file is:

```
$DATADIR/update_data.tar.gz
```

Note:

- All the files from the package with relative paths are deployed in a unique directory at the default path that is configured in the IoT Agent. The default path can be found in the `iotc-agent` configuration file, at agent host: `/opt/smarthub/iotc-agent/conf/iotc-agent.cfg`.

`agentDataDirPath` = `/opt/smarthub/iotcagent/data`

- Ensure that you provide appropriate access and execution rights to the files, if needed. You can provide permissions through the executables for the lifecycle phases.

- You can specify a relative or an absolute install path for the attachments. If you do not specify the install path, the **Package Management CLI** tool creates an install path for each attachment.

14.2 Lifecycle Phases

The lifecycle section defines the different lifecycle phases and the corresponding action to take for each phase. For the IoT Agent to locate an `action` executable after the payload is extracted, and to run the executable, the `action` path must match the `installPath` in the `attachments` section.

Or, the `action` path must point to an existing executable on the gateway. The specification file also specifies the external executables to run at each lifecycle phase.

The lifecycle phases are:

- `entrypoint`
- `verify`
- `execute`
- `**validate`
- `activate`
- `reset`

Note:

- You can attach executables to all lifecycle phases except the entry point phase. The executable for the entrypoint phase must be present on the Gateway's file system and ready to run.
- These lifecycle phases are optional.

If you use lifecycle phases, you cannot modify the phases or the order in which the phase actions are run. If you do not specify executables in the `action` field, then no action is performed and the phase is considered to pass successfully and the lifecycle moves to the next phase.

For example, if you do not provide a `verify.sh` executable in the **verify** phase, the package runs without verification (other than the default verification steps provided in the packaging format, such as checksum and RPM signatures), and moves to the **validate** state.

This process continues until the package moves to the **activate** phase. The phases **activate** and **reset** are mutually exclusive. The update is either activated or reset depending on the **validate** phase result.

Note:

- For all the executables that are attached for the action field, the IoT Agent sets the execute permission to (`700 / -rwx-----`) for the `iotc` user by default.
- If there are other executables listed in `packages/files/scripts` beside the executables that are specified in the action field, the author of the executables must manage the required permissions.

The `architecture` and `os` sections are strings that describe the operating system and architecture that the package is built for. If the `architecture` or `os` sections are not present or have empty values, the **Package Management CLI** tool detects the values.

These values are supplied to the **Package Management CLI** tool when building the tool itself. The **Package Management CLI** tool is available in the following variants. These variants are available in a downloadable file within the `package-cli.zip` file:

- OS = linux, Architecture = amd64
- OS = darwin, Architecture = 386
- OS = windows, Architecture = amd64
- OS = windows, Architecture = 386

Note: You cannot use a variant of the **Package Management CLI** tool that is not built for the specific system architecture or operating system. For example, you cannot use the Windows Package Management CLI tool on a Linux machine.

This way, the **Package Management CLI** tool detects the system architecture or operating system and populates them with the values that are built into the tool. The default operating system values that are built in for detection are Windows, MacOS, and Linux.

The tool defaults to `noos` if it is unable to detect an operating system. Similarly, the **Package Management CLI** tool defaults to `noarch` if it is unable to detect a system architecture.

14.3 Downloading the Package Management CLI Tool

This section lists the steps to download the **Package Management CLI** tool.

1. Log in to INFER™.
2. From the home screen, click the settings icon on the top right corner and click **Downloads**.
3. Under **Campaigns CLI**, download the **Package Management CLI** file to your local disk.
4. Extract the `package-cli.zip` file and run the `package-cli` file for your desired operating system.

14.4 Generating an IoTCP Package

Generate an `.iotcp` package, upload it to INFER™, and run campaigns using the package.

The package command contains two subcommands:

```
> ./iot-cli package
Package software for INFER IoT Center

Usage:
  package-cli package [command]

Available Commands:
  create      Generate an IoT Center package according to a package manifest.
  upload      Upload a created package to INFER IoT Center.

Flags:
  -h, --help  help for package

Use "package-cli package [command] --help" for more information about a command.
```

14.4.1 The Package Create Subcommand

The package create subcommand creates a package using a specification file. It contains a flag without any shorthand name:

```
> ./iot-cli help package create
Generate an IoT Center package according to a package
manifest.

Usage:
  package-cli package create <path to package.yml> [flags]

Flags:
  -h, --help help for create
      --no-approval Disables user approval before creation
  -o, --output string Set output path (default ".")
```

The create command has the following modification flags:

- `-o, --output` - Sets the output path for the package that is created.

The package create command requires a confirmation to create the package.

Example 1: Any input other than `y` stops the package creation process.

```
> ./iot-cli package create example-iotc-package/packagespec.yml

You are creating a package with:
Name: hello_iotcp
Version: 1.1.0
OS: linux
Architecture: noarch

File will be created as: hello_iotcp-1.1.0.linux.noarch.iotcp

Do you want to continue ? [y/n] y

Creating package hello_iotcp-1.1.0.linux.noarch.iotcp
```

Example 2: In this example, `y` is sent as an input to the command using bash here string `.`

```
> ./iot-cli package create example-iotc-package/packagespec.yml <<< y

You are creating a package with:
Name: hello_iotcp
Version: 1.1.0
OS: linux
Architecture: noarch
File will be created as: hello_iotcp-1.1.0.linux.noarch.iotcp

Do you want to continue ? [y/n]
Creating package hello_iotcp-1.1.0.linux.noarch.iotcp
```

Example 3: The `--no-approval` flag is present:

```
> ./iot-cli package create example-iotc-package/packagespec.yml --no-approval

You are creating a package with:
  Name: hello_iotcp
  Version: 1.1.0
  OS: linux
  Architecture: noarch
File will be created as: hello_iotcp-1.1.0.linux.noarch.iotcp
```

```
Creating package hello_iotcp-1.1.0.linux.noarch.iotcp
```

The **Package Management CLI** tool also supports pipes that do not require an approval. The approval flag is not required here:

```
> ./iot-cli package create
```

If the path to the yaml config is not passed as argument, you can use pipes to pass the yaml config file.

Usage with pipes: `cat package.yaml | iot-cli package create`

Usage with yaml parameter: `iot-cli package create test_pac.yaml`

For example:

```
cat example-iotc-package/package-spec.yaml | ./iot-cli package create
```

You are creating a package with:

```
Name: hello_iotcp
Version: 1.1.0
OS: linux
Architecture: noarch
```

File will be created as: `hello_iotcp-1.1.0.linux.noarch.iotcp`

```
Creating package hello_iotcp-1.1.0.linux.noarch.iotcp
```

14.4.2 Creating an IoTC Package

Use the following steps to create an IoTC package:

1. Ensure that you have created a specification file.
2. Download and install the Package Management CLI tool. You must have executable permissions to run this tool.
3. From the **Package Management CLI** tool, run the following command:

```
package-cli package create <path-to-spec>
```

Here, `<path-to-spec>` is the path to the `YML` file.

Optionally, you can specify an output file using the `-o` flag. By default, the current directory is used as the output path. The resulting file is named

```
`{name}-{version}.{os}.{architecture}.iotcp`.
```

1. Next, upload the package using the INFER™ UI or by using the **Package Management CLI** tool.

Run the `\$ package-cli upload package \<path to package> \<INFER IoT Host>` command. For example:

```
$ package-cli upload package UpdateVIPonGW-3.linux.noarch.iotcp https://<INFER IoT Host IP>
```

Note: The upload package command creates the package in the Root organization.

14.4.3 Uploading the IoT Package

This section lists the steps for uploading an IoT Package.

1. Download and install the **Package Management CLI** tool from the INFER™ UI.
2. The upload command contains two subcommands to handle the package and manifest uploads.

```
$ package-cli upload
Upload files to INFER IoT Center

Usage:
package-cli upload [command]

Available Commands:
package Upload a created package to INFER IoT Center.

Flags:
-h, --help help for upload

Use "package-cli upload [command] --help" for more information about a command.
```

3. Run the `\$ package-cli upload package <path to package> <INFER IoT Host>` command.

```
$ package-cli upload package myPackage.iotcp
https://<INFER IoT Host IP>
```

Note: The `\<INFER IoT Host>` must contain a valid schema (https:).

4. You are prompted to enter a user name and password. Ensure that the user credentials you enter has sufficient privileges to upload packages.

After the package uploads, the package's UUID appears on the UI.

14.5 Sample Script for Running a Campaign on a Thing Device

The package to update a Thing device contains scripts that are run on the gateway where the Thing device is connected.

To enable package script development, the Agent runs the package scripts with the **TARGET_THINGS** environment variable. This environment variable contains the space-separated Thing IDs that the campaign targets for updates.

Based on these Thing IDs, you as a script developer can obtain the required properties from the Agent's **DefaultClient** command-line tool.

14.5.1 Sample Campaign Script

This following sample script provides information about updating the IP cameras that are connected to a gateway:

```
#!/usr/bin/env bash
if [ -z "$TARGET_THINGS" ];
then
    echo "No cameras are provided"
    exit 0
fi
# convert target thing ids to array
camera_ids=("$TARGET_THINGS")
for camera_id in "${camera_ids[@]}"
do
```

```

    echo "Updating IP camera with device ID=$camera_id"

    # Get the required thing properties
camera_ip=`/opt/smarthub/iotc-agent/bin/
DefaultClient getproperties --device-id="$camera_id" --type=
custom --propertyname="IP"`
    # The get operation might fail, so appropriate error
handling can be added here.
    camera_ip_successfully_retrieved=$?
    echo "Camera IP: $camera_ip"
    curl http://${camera_ip}/cgi/UpdateFirmware
filename=firmware.bin
    update_result=$?

    if [ 0 -ne $update_result ]
    then
        failed_updates+=("$camera_id")
    fi
done

if [ ${#failed_updates[@]} -ne 0 ];
then
    echo "The update failed for: ${failed_updates[@]}"
    exit 1

fi
echo "Successful"
exit 0

```

In this example,

```
camera_ip=/opt/smarthub/iotc-agent/bin/DefaultClient get-properties --device-id="$camera_id"
```

gets the required properties of the IP camera such as IP address using the IP camera ID.

```
curl http://${camera_ip}/cgi/UpdateFirmwarefilename=firmware.bin
```

It sends the firmware updates to the IP cameras from the location mentioned in the script.

The following part of the script describes the error handling information when an update fails for one of the IP cameras:

```

if [ 0 -ne $update_result ]
then
    failed_updates+=("$camera_id")
fi
done

if [ ${#failed_updates[@]} -ne 0 ];
then
    echo "The update failed for: ${failed_updates[@]}"
    exit 1
fi

```

15 Working with Alerts & Notifications

This chapter explains the concepts and steps to configure your alerts and notifications in the INFER™ platform.

The Alerts module enables you to define alerts suited to various contexts.

15.1 What is an Alert?

An alert is a specific instance in time logged by when a asset meets the context and conditions specified in an alert definition.

- **Purpose:** Alerts are used in various contexts to convey to users critical or urgent information that requires immediate attention quickly and efficiently. They are designed to grab your attention and prompt you to take specific actions in response to a particular event or situation. Alerts are often used for important system or security-related messages.
- **Timing:** Alerts are immediate and intrusive by nature. They are meant to disrupt your current activity to ensure that you see and respond to the message promptly.
- **Content:** Alerts contain concise and critical information. They include warnings, error messages, emergency notifications, or important updates that require immediate action.
- **Persistence:** Alerts may stay on the screen until you dismiss them or take the required action. Additionally, alerts will continue to remain in **Active** status till the system determines that it can be canceled.

15.1.1 Asset Offline Alerts

You can create alert definitions on asset templates to trigger an alert when a asset does not ingest any metrics for a particular time duration.

Note: For a newly added asset that does not have any ingested metrics, at least two data points must be ingested before the absence of more metrics triggers a **Asset Offline** alert.

15.1.2 Searching Alerts

From the **Alerts & Notifications > Alerts** tab, you can search for alerts by their:

- Definition
- Update time range
- States: **ACTIVE**, **ACKNOWLEDGED**, or **CANCELLED**

15.1.3 Acknowledging Alerts

1. To acknowledge an active alert from the list of alerts, select the alert and scroll right and click on the vertical ellipsis against the selected alert. Click **Acknowledge**.

Select	Acknowledge	Severity	Asset Type	Asset	State	Last Modified (IST)	Actions
<input checked="" type="checkbox"/>		CRITICAL	Device	az-vm-bastion01	ACTIVE	Mar 29, 2024 12:03 PM	⋮
<input type="checkbox"/>		CRITICAL	Device	vm-containerapps01	ACTIVE	Nov 27, 2023 3:14 PM	⋮
<input type="checkbox"/>		CRITICAL	Device	vm-containerapps01	ACTIVE	Oct 17, 2023 6:39 AM	⋮
<input type="checkbox"/>		CRITICAL	Device	blr-lab-ubu01	ACKNOWLEDGED udaykiranginfer.local	Jan 31, 2023 12:46 PM	⋮
<input type="checkbox"/>		CRITICAL	Device	sea-lab-ubu01	ACTIVE	Oct 7, 2022 12:44 PM	⋮
<input type="checkbox"/>		CRITICAL	Device	OVH-US-Jumpserver	ACTIVE	Sep 29, 2022 7:46 AM	⋮
<input type="checkbox"/>		CRITICAL	Device	ovh-ekvg01	ACTIVE	Sep 29, 2022 7:38 AM	⋮

- To acknowledge multiple alerts, click multiple alerts and click the vertical ellipsis on the top of the UI page. Click **Acknowledge**. The alert's state changes to **Acknowledged** and the user name of the person who acknowledged the alert appears.

15.1.4 Alert Details

The Alerts Details page displays the entire information of the selected alerts on the **All Alerts** page. On this page, you can:

- Copy the Alert Definition ID
- Copy Asset ID
- Modify the Time Range of the asset generated and also view with a pictorial representation of its online or offline state

15.1.5 Alert History

You can view the alert history of an asset and know if an alert is new or an existing one. You can also view:

- Number of times the asset has raised this alert
- Identify the metric and value
- Time stamp when the alert was triggered

Select the alert definition and click the **History** tab. A graph indicating the alert states is also shown.

Alert Notifications are sent only if notifications are configured correctly. They are sent for both **ACTIVE** and **CANCELLED** states.

15.1.6 Alert Filter

You can filter an alert by its Alert Definition Name, Severity, Asset, and State.

15.1.7 Alert Date range

You can filter alerts based on a specific date range. The UI offers predefined options—ranging from the last 5 minutes to the last 30 days—as well as the ability to select a custom date range.

15.2 What is an Alert Definition?

An Alert definition is a grouping of unique symptoms and recommendations that you combine to identify problem areas and generate alerts.

An alert definition in INFER™ consists of:

- A asset template
- A asset metric/property
- A condition expression
- The number of times the condition must be true for a asset to trigger that alert.

For example, you can define an alert to trigger whenever the temperature of a asset exceeds 130 degrees. You can set a pre-defined notification definition in your alert definition to notify the users through email or a user-defined callback API whenever the alert is triggered.

Name	Severity	State	Resource Templates	Description	Organization	Updated (IST)
BLR-location	CRITICAL	Enabled	FileUploadTemplate	-	Smarthub	01/28/2025, 2:13 PM
CPU Threshold	CRITICAL	Enabled	FileUploadTemplate, Default Gateway Template	-	Smarthub	01/28/2025, 2:13 PM
memory usage	CRITICAL	Enabled	FileUploadTemplate	-	Smarthub	01/28/2025, 2:13 PM
Camera 1.101 Down	WARNING	Enabled	Default Gateway Template	-	Smarthub	01/28/2025, 2:12 PM
Zoom Room Offline	INFO	Enabled	Default Gateway Template	-	IoT Inc	01/28/2025, 2:08 PM
Alert-Axis Camera	CRITICAL	Enabled	Default Gateway Template	-	IoT Inc	01/23/2025, 5:09 PM

15.3 Creating an Alert Definition

This section lists the various alert definition types you can create using the Alerts module in INFER™.

1. **Creating an Alert Definition across multiple asset templates:** You can create a single alert definition that works across multiple asset templates. When you create alert definitions for multiple asset templates, ensure that the metrics or properties for the alert definition symptom is common across all the asset templates that you have selected.
2. **Creating an alert definition for single asset template with command definition (with arguments):** You can create an alert definition for a single asset template and select command definition (with arguments) that is executed when the alert is triggered.
3. **Creating an Alert Definition for assets in an Advanced Search Query:** If you have saved an advanced search query for assets, you can create an alert definition for those assets that are part of that saved query.
4. **Creating a Threshold Alert Definition:** You can also create a threshold alert definition for a single asset template or across multiple asset templates from the Console.
5. **Creating an Offline Alert Definition:** You can create an offline alert definition from the Console to trigger asset offline alerts if the Server does not receive metrics or system property values for a specified duration.

Prerequisite: To create an alert definition in INFER™, you must have the `CREATE_ALERT_DEFINITION` permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ UI, navigate to **Alerts & Notifications > Alert Definitions**.
2. Click **CREATE**. The **Create Alert Definition** wizard appears as shown below:

Create Alert Definition

1 Details

2 Templates

3 Condition

4 Recommendation

5 Notification Definition

6 Commands

7 Review

Details

This step consists of basic details of the Alert definition

Name *

CPU Temp@45

Resource *

Asset

Description

Tracks CPU Temperature Beyond 45 degrees

CANCEL NEXT

3. Under **Details**, enter a **Name** and **Description** of your alert.
4. Click **NEXT**.
5. Under **Select Asset > TEMPLATES**, select one or more asset templates.

Note:

- You can create a single alert definition that works across multiple asset templates.
 - The alert definition can either be Template-based or Saved Search-based but not both.
 - Ensure that the metrics or properties for the alert definition symptom is set common across all the asset templates that you have selected.
6. Next, click **SAVED SEARCH**. Use the **Select** drop-down menu to search for previously searched asset templates.

Note: If you have a saved advanced search query for assets, you can create an alert definition for those assets that are part of the query.

7. Click **PREVIEW** to review values of the selected asset template.
8. Click **NEXT**.

15.3.1 Creating an Offline / Threshold Alert Definition

1. Under **Condition**, choose between setting up **THRESHOLD** and **OFFLINE** alert definitions.

Note:

- Threshold alert definition is defined by a trigger condition on Metric/Property.

- Offline alert definition is defined by time interval
2. Under **THRESHOLD > Symptom**, from the drop-down menus, add conditions that trigger your alert by selecting the values for **Metric/Property**, **Condition**, **Severity**, and **Trigger Count**.

Note:

- Threshold alert definition is defined by a trigger condition on Metric/Property.
 - You can create a threshold alert definition for a single asset template or across multiple asset templates.
 - Ensure that the selected metric or property exists on all selected asset templates.
3. Under **Symptom**, select a metric or system property, its condition, and enter the metric value to trigger the alert.

Note:

- Since system properties have string values, the allowed conditional operators are **=** and **!=**
 - For Metrics of type Boolean, the values are case-sensitive and can be either **FALSE** or **TRUE**
4. From the **Severity** drop-down menu, select the severity of the alert:

Note: The alert severity types are:

- CRITICAL - Red
 - WARNING - Orange
 - INFO - Blue
 - NORMAL - Defines the normal threshold for the alert to cancel.
5. Click **+ Add** icon to add multiple conditions and severity options to the symptom.
 6. From the **Trigger Count** drop-down menu, select the number of times the condition must be met to trigger the alert.

Note:

- For system property-based alerts, it is recommended to set the trigger count to 1.
 - The alert definition is either Threshold-based or Offline-based but not both.
7. Next, click **OFFLINE**.

Note:

- You can trigger asset offline alerts if the INFER™ Server does not receive metrics or system property values for a specified duration.
 - You can create asset offline alert definitions only for the allowed metrics that are on the asset template.
 - Offline alert definition is defined by time interval.
8. Under **Check interval for absence of metrics or system properties**, enter the duration in minutes that the Server must wait to receive metrics and system property values from a asset before triggering the alert.
 9. Under **Recommendation**, enter the action that the technician or administrator must take when the alert is triggered.
 10. Click **NEXT**.

15.3.2 Select Alert Notifications

1. Under the **Notification** tab, from the **Select Active Alert Notification** and **Select Cancel Alert Notification** drop-down menu, select a valid notification definition that will be sent when an Alert is triggered.
2. Click **NEXT**.

3. Under **Commands**, click **Enable Commands** switch to select the commands that will be executed when the alert is triggered.
4. Next click **+ Add** icon and select the desired command from the drop-down menu.
5. Specify the parameters under **Argument Name** and **Argument Value**.
6. Click **DONE**.
7. Click **NEXT**.
8. Under **Review**, review the new alert definition information you entered and click **SAVE**. You have successfully created a new alert definition.

15.4 Editing Alert Definitions

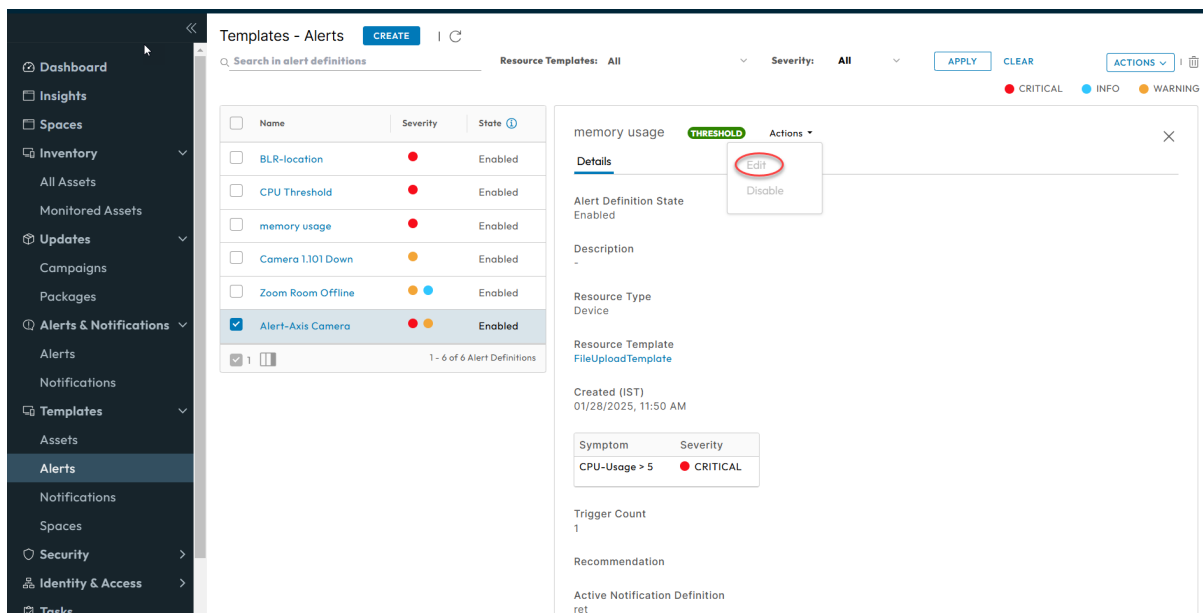
When you edit the values of an alert definition such as **Template**, **Symptom**, or **Trigger Count**, the system cancels all active and acknowledged alerts triggered by the previous alert definition.

However, when you change the alert severity, the existing alerts retain the old severity and the new alerts use the new severity.

Changing the informational values of the alert definition such as name, description, or recommendation does not affect existing alerts.

Prerequisite: To edit an alert definition in INFER™, you must have the `EDIT_ALERT_DEFINITION` permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ UI, navigate to **Templates* > Alerts**.
2. From the listed alert definitions, click the alert definition which you desire to edit. The following tab appears as shown below:



3. Under **Actions** drop-down menu as highlighted above, click **Edit**.
4. The **Edit Alert Definition** wizard appears.
5. Edit the existing alert definition details and click **SAVE**. You have successfully edited an alert definition.

Note: If you change the **Condition** of your alert definition, all active alerts from the previous condition are automatically canceled.

15.5 Disabling Alert Definitions

Prerequisite: To disable an alert definition in INFER™, you must have the EDIT_ALERT_DEFINITION permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ UI, navigate to **Templates > Alerts**.
2. From the listed alert definitions, click the enabled alert definition which you desire to disable.
3. Under **Actions** drop-down menu, click **Disable**.
4. The **Disable Alert Definition** pop-up appears as shown below:

Disable Alert Definition

You are about to Disable the Alert Definition(s) listed below.
All active alerts for definition(s) listed below will be cancelled.

Provide a reason for this change*

To enable new definition

☒ Camera High Temperature Sensor 1 - Enabled

☒ 1

CANCEL **DISABLE ALERT DEFINITION**

5. Enter the reason for the change and click **DISABLE ALERT DEFINITION**. You have disabled the alert definition successfully.

Note: If you change the condition of your alert definition, all active alerts from the previous condition are automatically canceled.

15.6 Enabling Alert Definitions

Prerequisite: To enable an alert definition in INFER™, you must have the EDIT_ALERT_DEFINITION permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ UI, navigate to **Templates > Alerts**.
2. From the listed alert definitions, click the disabled alert definition which you desire to enable.
3. Under **Actions** drop-down menu, click **Enable**.
4. The **Enable Alert Definition** pop-up appears as shown below:

Enable Alert Definition

You are about to Enable the Alert Definition(s) listed below.

Provide a reason for this change*

Fits current requirement

☒ Camera High Temperature Sensor 1 - Disabled

☒ 1

CANCEL ENABLE ALERT DEFINITION

5. Enter the reason for the change and click **ENABLE ALERT DEFINITION**. You have enabled the alert definition successfully.

15.7 What is a Notification?

A Notification is an email/http warning message sent to grab the recipient user's attention quickly and provide relevant information to make informed decisions or take appropriate actions. Using http makes it possible to integrate with external ticketing systems, integrate with an SMS provider service etc.

The Notifications module acts as a primary interface for all HTTP and email (SMTP) notifications from the Server. All the other services communicate with the notifications service to send notifications to the external servers.

The Notifications module enables you to receive timely notifications without logging in to the systems, or without providing an integration point into the existing monitoring systems.

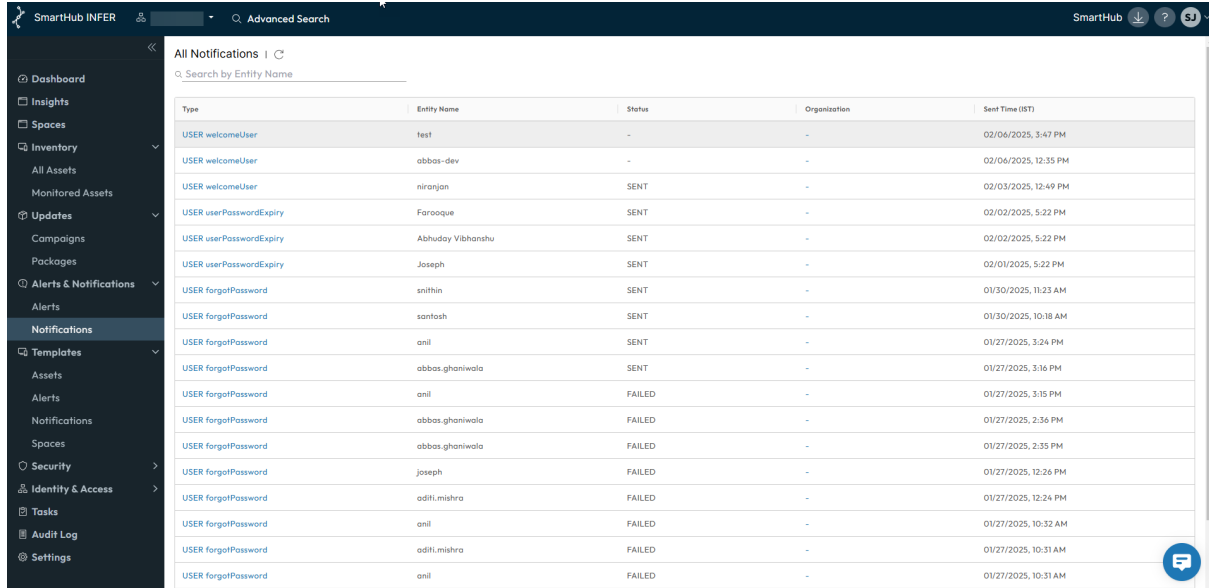
- **Purpose:** Notifications are used to provide you with general information, updates, or reminders. They are used to keep you informed about various system events or changes, and upcoming tasks.
- **Timing:** Notifications can be scheduled or delivered at a convenient time for the user. They are less intrusive and are often shown in a non-disruptive manner.
- **Content:** Notifications can contain a wide range of information, from reminders, to specific updates. They are generally more varied in content and are not necessarily urgent.
- **User Interaction:** Notifications may or may not require immediate interaction. Users can choose when and how to respond to notifications. They can dismiss them or choose to engage with the content later.
- **Persistence:** Notifications are less persistent and can be dismissed or archived by the user, or they may automatically disappear after a certain period if left unattended.

15.7.1 Viewing Notifications

You can use the Notifications tab as shown below to view email and REST-based notifications.

Prerequisite: To view notifications in INFER™, you must have the VIEW_NOTIFICATION_INSTANCE permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ UI, navigate to **Alerts & Notifications > Notifications**. The **All Notifications** page appears as shown below:



Type	Entity Name	Status	Organisation	Sent Time (ST)
USER welcomeUser	test	-	-	02/06/2025, 3:47 PM
USER welcomeUser	abbas-dev	-	-	02/06/2025, 12:35 PM
USER welcomeUser	niranjan	SENT	-	02/03/2025, 12:49 PM
USER userPasswordExpiry	Farooque	SENT	-	02/02/2025, 5:22 PM
USER userPasswordExpiry	Abhoday Vibhanshu	SENT	-	02/02/2025, 5:22 PM
USER userPasswordExpiry	Joseph	SENT	-	02/01/2025, 5:22 PM
USER forgotPassword	snithin	SENT	-	01/30/2025, 11:23 AM
USER forgotPassword	santosh	SENT	-	01/30/2025, 10:18 AM
USER forgotPassword	anil	SENT	-	01/27/2025, 3:24 PM
USER forgotPassword	abbas.ghaniwala	SENT	-	01/27/2025, 3:16 PM
USER forgotPassword	anil	FAILED	-	01/27/2025, 3:15 PM
USER forgotPassword	abbas.ghaniwala	FAILED	-	01/27/2025, 2:36 PM
USER forgotPassword	abbas.ghaniwala	FAILED	-	01/27/2025, 2:35 PM
USER forgotPassword	joseph	FAILED	-	01/27/2025, 12:26 PM
USER forgotPassword	aditi.mishra	FAILED	-	01/27/2025, 12:24 PM
USER forgotPassword	anil	FAILED	-	01/27/2025, 10:32 AM
USER forgotPassword	aditi.mishra	FAILED	-	01/27/2025, 10:31 AM
USER forgotPassword	anil	FAILED	-	01/27/2025, 10:31 AM

2. Click the desired notification to view more information about it.

15.8 What is a Notification Definition?

A Notification Definition refers to the description or specification of how the format, content, and behavior of email and REST-based notifications should be structured and delivered within INFER™.

Notification definitions also contain details such as the:

- Notification's destination
- Sender Information
- The number of times to retry sending

15.9 Creating a Notification Definition

This section lists the steps to create a notification definition in INFER™.

Prerequisite: To create a new notification definition in INFER™, you must have the CREATE_NOTIFICATION_DEFINITION permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ UI, navigate to **Alerts & Notifications > Notification**.
2. Click **CREATE**. The **Create Notification Definition** wizard appears as shown below:

3. Under **Name**, enter a name for your alert.
4. Under Description, enter a brief description of your alert.
5. Click **NEXT**.
6. Under **Settings > Type**, from the drop-down menu, choose the notification type.
7. Under the **Recurrence** tab, select the required interval and click **Next**.
8. Review the content and click **Save**.

15.9.1 Email Notification

1. In step 6. if you chose **Email Notification**, under **Notification Categories**, from the drop-down menu, choose your desired notification category.
2. Under **Advanced Settings**, the fields carry default values. However, these can be overwritten. You can revert to default values by deleting the overwritten values.
3. Enter the values for **Sender Name**, **Base URL**, **Sender Email Address**, and **Email Subject**.
4. Under **--Insert field--**, use the drop-down to select the desired option.
5. Click **NEXT**.
6. To configure your notification to reoccur, under **Recurrence**, click the checkbox against **Recurrence notification**
7. Under **Recurrence Interval**, specify the **days**, **hours**, and **minutes**.
8. To configure the maximum number times the notification has to reoccur, under **Max Recurrence Count**, enter between 1 - 100 recurrence count.
9. Click **NEXT**.
10. Under **Review**, review the notification definition information you entered and click **SAVE**. You have successfully created a new notification definition.

15.9.2 REST-based Notifications

1. In step 6. if you chose **REST Notification**, under **Notification Categories**, from the drop-down, choose your desired notification category.

2. Click the checkbox against **Secure Protocol (Secure (TLS) is recommended)**
3. Under **Host URL**, enter the host URL.

Note: The default port number is 443.

4. Under **Certificate**, paste the certificate details.
5. Under **Authentication Type > Basic**, from the drop-down, select your desired authentication type.

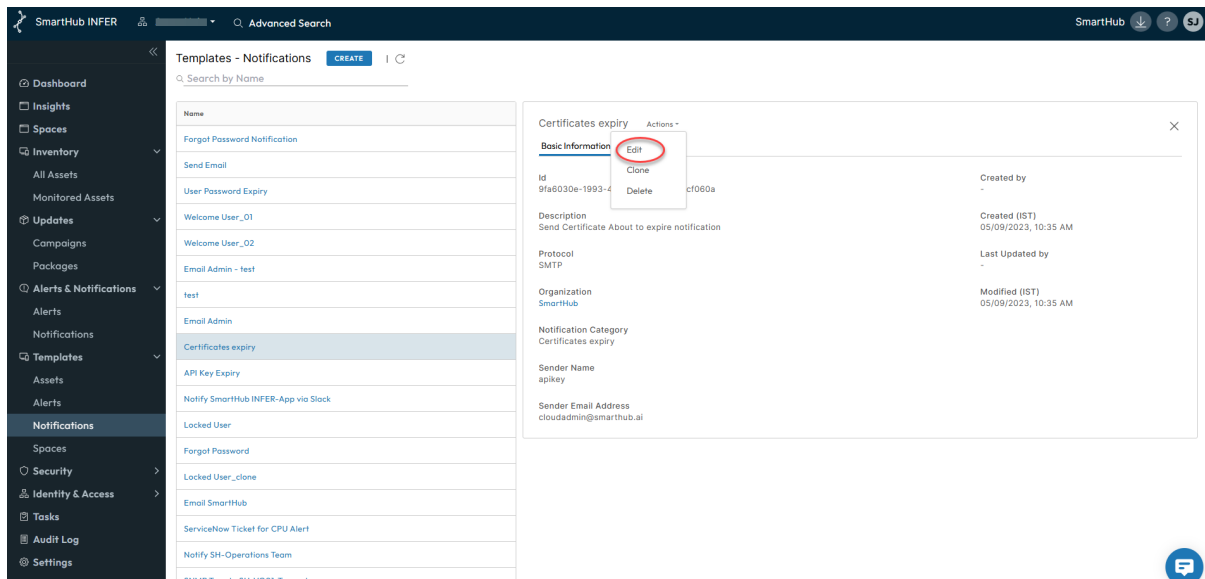
Note: Auth-based REST Server is recommended.

6. Under **Basic**, enter the Username and Password.
7. Under **Advanced**, if required, click the checkbox against **Retry Schedule**.
8. Under **Retry Interval**, specify the **hours**, **minutes**, and **Seconds**.
9. Under **Request Timeout**, specify the **minutes**, and **Seconds**.
10. Under **Max Retry Count**, specify the retry count.
11. Under **Headers**, click **+ Add New Header** to add a new header.
12. Specify the **Header Name** and **Header Value** parameters, and click **DONE**.
13. Next, click the checkbox against **Use Default Rest Template** to use the default REST Template.
14. Else, under **Body Template**, edit the desired values.
15. Under **--Insert field--**, use the drop-down to select the desired option.
16. Under **Validate Response**, enter the response string.
17. Click **NEXT**.
18. Under **Link**, setup linked notifications for sent notifications.
19. Under **On success, send additional notification**, from the drop-down, select the desired option.
20. Under **On failure, use alternate notification definition**, if you want to send another notification to get notified of the nature of the failure of the original notification along with its notification data, from the drop-down, select the desired option.
21. Under **On failure, send debug information using**, if you want to send another notification upon failure to know why the previous notification failed, from the drop-down, select the desired option.
22. Click **NEXT**.
23. Under **Review**, review the notification definition information you entered and click **SAVE**. You have successfully created a new notification definition.

15.10 Editing Notification Definitions

Prerequisite: To edit a notification definition in INFER™, you must have the EDIT_NOTIFICATION_DEFINITION permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ UI, navigate to **Templates > Notifications**.
2. From the listed notification definitions, click the notification definition which you desire to edit. The following tab appears as shown below:



Note: The **Basic Information** displays key details such as the notification ID, description, creation date, and other essential information used to define a notification. Similarly, the **Used by** tab lists the alert definitions that are using that notification definition. You can click on any alert definition to view the alert definition details.

4. Under **Actions** drop-down menu as highlighted above, click **Edit**. The **Edit Notification Definition** wizard appears.

Note: **Type** and **Notification Categories** parameters are not editable.

4. Edit the notification definition details and click **SAVE**. You have successfully edited a notification definition.

15.11 Cloning Notification Definitions

Prerequisite: To clone a notification definition in INFER™, you must have the CREATE_NOTIFICATION_DEFINITION permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ UI, navigate to **Templates > Notifications**.
2. From the listed notification definitions, click the notification definition which you desire to clone.
3. Under **Actions** drop-down menu, click **Clone**. The **Create Notification Definition** wizard appears.

Note: **Type** and **Notification Categories** parameters are not editable.

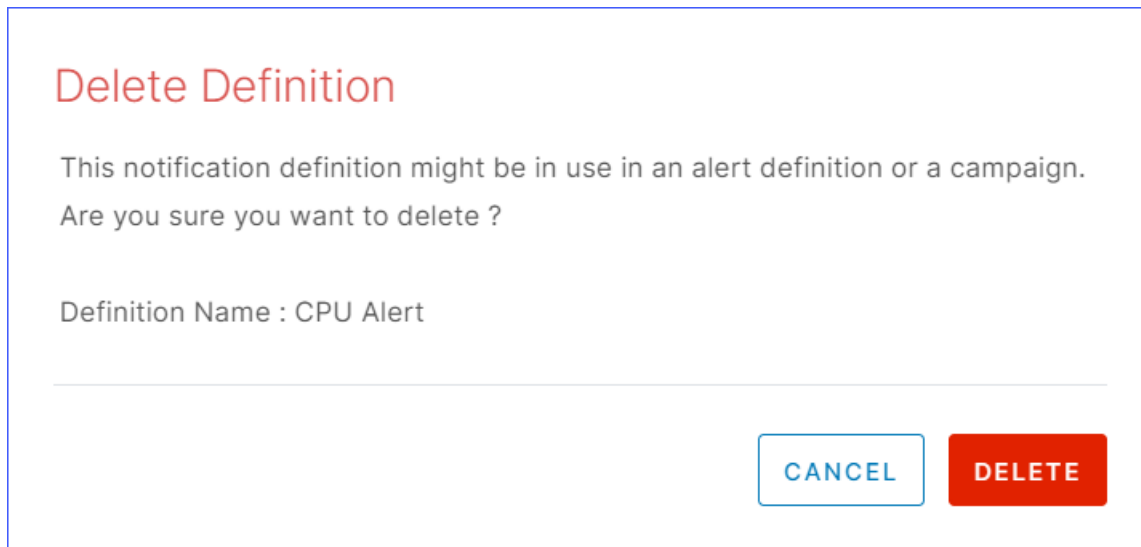
4. Enter new notification definition details as required and click **SAVE**. You have successfully cloned a notification definition.

15.12 Deleting Notification Definitions

Prerequisite: To delete a notification definition in INFER™, you must have the EDIT_NOTIFICATION_DEFINITION permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ UI, navigate to **Templates > Notifications**.
2. From the listed alert definitions, click the enabled alert definition which you desire to disable.
3. Under **Actions** drop-down menu, click **Disable**.

4. The **Delete Notification Definition** pop-up appears as shown below:



The image shows a 'Delete Definition' dialog box. At the top, the title 'Delete Definition' is in red. Below it, a message states: 'This notification definition might be in use in an alert definition or a campaign. Are you sure you want to delete ?'. Underneath, it says 'Definition Name : CPU Alert'. At the bottom right, there are two buttons: a blue 'CANCEL' button and a red 'DELETE' button.

Note: The notification definition you have selected might be in use in an alert definition or a campaign.

5. Click **DELETE**. You have deleted the notification definition successfully.

15.13 Sending Notifications to ServiceNow

You can send notifications from INFER™ to a **ServiceNow**. When an alert is generated for a asset, it creates an incident in the ServiceNow instance.

This section lists the steps to integrate INFER™ with ServiceNow instance.

Prerequisite: You must have access to the following instances:

- INFER™ Console
- ServiceNow instance

15.13.1 Creating a Notification Definition

1. Navigate to **Templates > Notifications**.
2. Under **Templates - Notifications**, click **CREATE**.
The **Create Definition** wizard appears.
3. Under **Details**, enter a name for the notification definition, enter an optional description, and click **NEXT**.
4. Under **Settings**, select the **Type** as **REST Notification**.
5. Under **Notification Categories**, and select the device alert. Enable **Secure Protocol**.
6. Under **Host URL** of the ServiceNow instance, enter the URL. For example, dev79872.servicenow.com. Enter the port number as 443.
7. In the URL field, append the URL with the path /api/now/table/incident.
8. Under **Certificate**, copy the security certificate, that is the Root CA from the ServiceNow browser and paste it in the Certificate text box.
9. Under **Authentication Type** drop-down menu, select **Basic**, and enter your ServiceNow credentials.
10. Under **Advanced Settings**, under **Headers**, click **+ Add New Header**, and enter the following values:

- `Content-type - application/json`
- `Host - <instance_id>.service-now.com for e.g: dev196221.service-now.com`

11. Click **DONE**.

12. Click **NEXT**.

Note: ServiceNow provides multiple tables to which you can insert or create a record. In this example, we use the **Incident** table to create a record. To view the full list of tables in ServiceNow, go to the ServiceNow instance and navigate to REST API Explorer.

13. Under **Body Template**, enter the keys to be populated in ServiceNow. You can derive the keys from the ServiceNow instance. The following example illustrates a sample body template:

```
{
  "caller_id": "Test User",
  "short_description": "Notification for Alert
  ${alertState}",
  "description": "This is an automated notification from SmartHub INFER IoT
  ↵ Center.
  \n\n Device Id :
  ${deviceId}, \n deviceTemplateId:
  ${deviceTemplateId}, \n Alert Name :
  ${alertTemplate}, \n Alert State : ${alertState}, \n
  Severity : ${alertSeverity}, \n Recommendation :
  ${recommendation}, \n Alert Definition ID :
  ${alertDefinitionId}, \n Metric Value : ${lambda}.
  \n\n To view additional details, go to the SmartHub INFER IoT Center Server."
}
```

14. Click **NEXT**.

15. On the Link page, you have an option to select a notification:

- Send a notification when there is a success
- Send a notification when there is a failure and you can use an alternate notification definition.
- Send a notification when you want to debug any sort of error.

16. Review the details that you have entered and click **SAVE**.

Note: ServiceNow provides multiple tables to which you can insert or create a record. In this example, we use the Incident table to create a record. To view the full list of tables in ServiceNow, go to the ServiceNow instance and navigate to REST API Explorer.

You have successfully integrated with ServiceNow. When you associate an alert definition with this ServiceNow notification definition, ServiceNow files an incident whenever an alert is triggered.

15.14 Sending Notifications to Microsoft Teams

This section lists the steps to send notifications from INFER™ to a channel in **Microsoft Teams**.

15.14.1 Collecting the required information from Microsoft Teams

1. Login to your **Microsoft Teams** Application and navigate to **Teams** tab on the left. Select the appropriate **Team** from the list and then select the appropriate **Channel**.
2. Click on the 3 dots ... next to channel name and select **Get email address**.
3. Click on **advanced settings** and ensure that one of these two options are selected.

- **Anyone can send emails to this address**
- **Only email sent from these domains:**

When selecting this option, add `smarthub.ai` in the text field below.

4. Copy the **email address** portion which will be of the form:

`38773f3.yourdomain.com@xx.teams.ms`

5. You will be using this **email address** in the next set of steps.

15.14.2 Setting up Notification Definitions for Teams

Prerequisite: You must have the `CREATE_NOTIFICATION_DEFINITION` permission to perform this operation.

1. On the INFER™ UI, navigate to **Templates > Notifications**.
The **Templates - Notifications** page appears.
2. Click **CREATE**.
The **Create Definition** wizard appears.
3. In the **Details** step, enter the following details:
 - **Name:** Notification definition name.
 - **Description:** Enter a brief description about the notification definition.
Click **Next**.
4. In the **Settings** step, enter the following information:
 - **Type:** Select the notification type as **Email Notification**.
Enter the following information:
 - **Recipient Email Address:** Enter the email address of the channel that was copied from **Microsoft Teams**, in the previous set of steps.
 - Click **Advanced Settings** to edit the following:
 - ★ Edit the sender name, sender email address, email subject
 - ★ Customize the email template to your needs.
 - Click **Next**.
5. You can setup the **Recurrence** step as required. For more information, see [Creating a Notification Definition](#).
Click **Next**.
6. Under **Review**, review the information and click **SAVE**.
7. Using the steps listed in the [What is an Alert Definition?](#) section, **Create** or **Modify** an **Alert Definition** to use the newly created **Notification Definition**.
8. When the Alert conditions are met, you will receive the notification in your **Microsoft Teams** channel.

You have successfully setup notifications to be sent to Microsoft Teams.

15.15 Sending Notifications to Slack

This section lists the steps to send notifications from INFER™ to a channel in **Slack**.

15.15.1 Setting up Incoming Webhooks in your Slack Workspace

1. Login to your **Slack** workspace in a browser and follow the instructions in [Sending messages using incoming webhooks](#) to setup your incoming webhook.

2. You will need the following items from the setup:

- **Webhook URL**

It will look similar to

```
https://hooks.slack.com/services/T000000000/B000000000/XXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

- **Root Certificate for slack.com**

Using a browser, download the `.pem` file for the Global Root CA used by *.slack.com. This certificate will be used by INFER™ to validate the identity of the webhook.

15.15.2 Setting up Notification Definitions for Slack

Prerequisite: You must have the CREATE_NOTIFICATION_DEFINITION permission to perform this operation.

1. On the INFER™ UI, navigate to **Templates > Notifications**.

The **Templates - Notifications** page appears.

2. Click **CREATE**.

The **Create Definition** wizard appears.

3. In the **Details** step, enter the following details:

- **Name:** Notification definition name.
- **Description:** Enter a brief description about the notification definition.

Click **Next**.

4. In the **Settings** step, enter the following information:

- **Type:** Select the notification type as **Rest Notification**.

Enter the following information from the information gathered in the previous section:

- Enable **Secure Protocol**.
- Enter `hooks.slack.com` next to **https://**.
- Leave `443` as-is. This is the HTTPS port number.
- After `443`, enter the remaining portion of the webhook starting with `/services/T...`.
- In the **Certificate** box enter the contents of the Root CA certificate `.pem` file for slack.com (collected in the previous section).
- Set the **Authentication Type** to `No Authentication`, as the webhook embeds the authentication token already.
- Click on **Advanced Settings** and add the following row under **Headers** by clicking **Add New Header**. **Header Name** is `Content-type` and **Header Value** is `application/json` and click **Done**
- Uncheck the **Use Default Rest Template** and enter the following text as **Body Template**.

```
{
  "text": "Alert ${alertTemplate} in ${alertState}
for device ${deviceName}.
\\n Description: ${description} \\nRecommendation:
${recommendation}\\n"
}
```

You can modify the **Body Template** to include other fields by picking them from **Insert Field** drop-down.

You can also use advanced formatting in the **Body Template** JSON based on what is supported by Slack as described in the above URL.

- Click **Next**.

5. You can setup additional notifications in the **Link** step as required. For more information, see [Creating a Notification Definition](#). Click **Next**.
6. Under **Review**, review the information and click **SAVE**.
7. Using the steps provided in the [Creating an Alert Definition](#) section, create or modify an **Alert Definition** to use the newly created **Notification Definition**.
8. When the Alert conditions are met, you will receive the notification in your chosen **Slack** channel.

You have successfully setup notifications to be sent to a particular Slack Channel.

15.16 Sending Notifications to Smartsheet

This section lists the steps to send notifications from INFER™ to add a row to a particular sheet in **Smartsheet**.

15.16.1 Collecting the required information from Smartsheet

1. Login to your **Smartsheet** application in a browser and follow the instructions detailed in [Generate an API key](#) to generate your api key. You will be using this api-key to authenticate with Smartsheet's account.
2. Create a new sheet (or open an existing one), and go to **File > Properties**. Keep the sheet ID handy. You will need this to identify the sheet where you wish to add a row.
3. Get the column-ids for all the columns you like to populate. This is essential for knowing which column to add information while adding a row. The column-ids can be fetched by accessing this [api](#). You can also use API tools like [Postman](#) to do this.
4. You will need the following items from the setup:
 - **Root Certificate for api.smartsheet.com** Using a browser, you can download the `.pem` file for the Global Root CA used by api.smartsheet.com. This certificate will be used by INFER™ to validate the identity of the API.

15.16.2 Setting up Notification Definitions for Smartsheet

Prerequisite: You must have the CREATE_NOTIFICATION_DEFINITION permission to perform this operation.

1. On the INFER™ UI, navigate to **Templates > Notifications**. The **Templates - Notifications** page appears.
2. Click **CREATE**. The **Create Definition** wizard appears.
3. In the **Details** step, enter the following details:
 - **Name:** Notification definition name.
 - **Description:** Enter a brief description about the notification definition. Click **Next**.
4. In the **Settings** step, enter the following information:

- **Type:** Select the notification type as **Rest Notification**.

Enter the following information from the information gathered in the previous section:

- Enable **Secure Protocol**
- Enter `api.smartsheet.com` next to **https://**
- Leave `443` as-is. This is the HTTPS port number.
- After `443`, enter the remaining portion of the api, i.e. `/2.0/sheets/{sheet-id}/rows` (replace sheet-id collected in the previous section).
- In the **Certificate** box enter the contents of the Root CA certificate `.pem` file for api.smartsheet.com (collected in the previous section).
- Set the **Authentication Type** to `No Authentication`; you will use headers to add the authentication token.
- Click **Advanced Settings** and add the following rows under **Headers** by clicking **Add New Header**. **Header Name** is `Content-type` and **Header Value** is `application/json`, **Header Name** is `Authorization` and **Header Value** is `Bearer {api-key}` (api key collected from previous section), and click **Done**.
- Uncheck the **Use Default Rest Template** and enter the following text as **Body Template**.

```
[
{
  "cells": [
    {
      "columnId": "column-id1",
      "value": "${alertState}"
    },
    {
      "columnId": "column-id2",
      "value": "${description}"
    },
    {
      "columnId": "column-id3",
      "value": "${deviceName}"
    }
  ]
}
]
```

5. You can modify the **Body Template** to include other fields by picking them from **Insert Field** drop-down. Click **Next**.
6. You can setup additional notifications in the **Link** step as required. For more information, see [Creating a Notification Definition](#). Click **Next**.
7. Under **Review**, review the information and click **SAVE**.
8. Using the steps provided in the [Creating a Notification Definition](#) section, create or modify an **Alert Definition** to use the newly created **Notification Definition**.
9. When the Alert conditions are met, you will receive the notification in your **Smartsheet** as a newly added row.

You have successfully setup notifications to be sent to a particular Smartsheet.

16 Security

This chapter explains the assets' security concepts and methods to secure your asset in the INFER™ platform.

16.1 Working with Certificates

This section explains how INFER™'s Certificate module uses device certificates to enhance security, ensure device authentication, encrypt communications, and manage device identities effectively.

The Certificate module is INFER™'s conduit to help you to assign certificates for Edge assets similar to provisioning packages in a Campaign.

At its core, the Certificates module is managed by two key services:

1. Identity and Access Management service
2. Device Management service

Essentially, before you configure an Edge system, Root and entity certificates must be imported into INFER™ and then assigned to the assets at the Edge.

The functions of certificates in INFER™ are multifold to enable edge administrators to import certificates into INFER™ and deliver them securely to the edge. The Infer Agent and adapters can use this to configure the edge to use the certificate for a specific purpose.

INFER™ allows you to import certificates into INFER™ and assign and unassign certificates to assets. Certificates are issued by a [Certificate Authority](#) (CA) for a certain time period. These entity certificates that are to be assigned to assets will also include its key pair. The key pairs are not accessible to end users once imported and are only provided to the assigned assets at the edge.

A certificate becomes invalid due to time stamp expiry: INFER™ sends an email notification to the certificate owners's group (including Organization Administrators and System Administrators) 30 days, 7 days, and 1 day before the token's expiration date.

16.1.1 Certificate States

Once created, certificates pass through the following states:

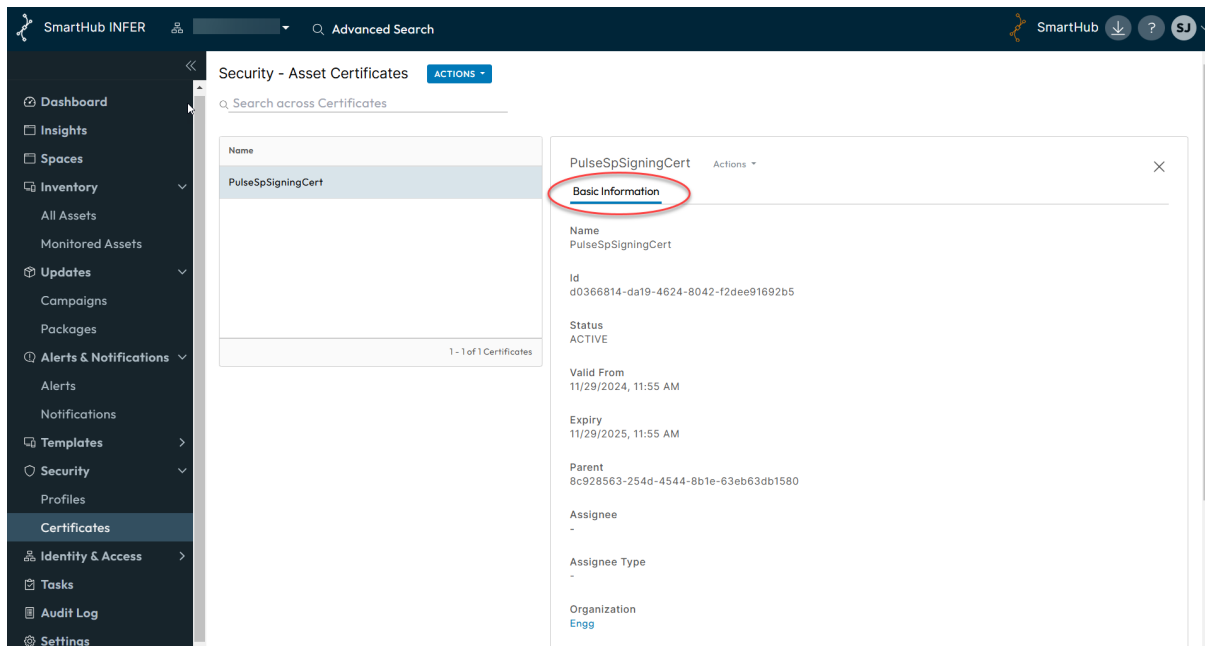
- Certificate in active use.
- Certificate disabled by the user.
- Certificate which has outlived its tenure.

16.1.2 Viewing Certificates

This section lists the steps to view the list of device certificates and their details present within INFER™.

Prerequisite: To view a certificate in INFER™, you must have the VIEW_CERTIFICATE permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ UI, navigate to **Security > Certificates**. The **Security - Asset Certificates** page appears.
2. Click your desired certificate. The certificate details appear under **Basic Information** tab.



When you import a certificate for the first time, INFER™ will not automatically trust it. Therefore, it is crucial to import the Root and CA Intermediate certificates. The chain will include the Root and any number of Intermediate CA certificates.

When you import a certificate into INFER™, it will trust the Intermediate Certificate after verifying it with its unique private key.

Remember to import the Root certificate first, followed by the Intermediate certificate. You can also import multiple Intermediate certificates if needed.

Note that you import root first and then Intermediate certificate. And you can have multiple intermediate certificates.

16.2 Importing CA Certificate

1. On the INFER™ UI, navigate to **Settings > Certificates**.
2. Select Certificates tab, under **ACTIONS** drop-down menu, click **Import Certificate**. The **Import Certificate** pop-up appears.
3. Under **Prefix**, enter a unique identifier for the certificates you are importing.
4. Under **Import Certificate**, click **UPLOAD CERTIFICATE** and select the certificate.
5. Click **IMPORT**. The certificate is imported into INFER™ **Settings > Certificates** list.

Note: The **Security - Certificates** page lists asset certificates, whereas, **Settings > Certificates** lists Root CA and Intermediate certificate.

16.3 Creating a Certificate Signing Request (CSR)

You can create a CSR for either an existing asset template or for a new asset. The following procedure provides steps to create a CSR for a new asset.

1. On the **Templates > Assets**, click **Create**.
2. Enter a valid **Template Name**, under the **Select Asset Type**, you can either select a **Gateway** or **Thing**.
3. Click **Next**.
4. Under the **Properties** tab, scroll down to **Custom Properties** and click **+ Add**.

5. Enter a valid Common name and click **Done**.
6. Click **Next**.
7. On the **Certificate Signing Request** wizard page, enter a **CSR Template Name**.
8. Select either **2048** or **4096** from the **Bits** drop-down menu.
9. Under the **Subject** section, associate a space template to a *Country*, *State* and *Locality* and it's respective attribute values for the CSR from the drop-down menus.
10. Enter a valid name for **Organization Name**, and **Organization Unit**.
11. Select the property for *Common Name* that you created under the Custom Properties from the **Common Name** drop-down menu.
12. (Optional) Under the **Subject Alternative Name**, if you select the **IP address** of the asset that is deployed from the drop-down menu, then select a DNS name in the next step and click **Add**.
13. (Optional) Under the **DNS-Name**, select the custom property of the asset selected and click **Add**.
14. Click **Next** to enter more details about the certificate, review the changes and click **Save**.
15. To validate the entries, navigate to the asset template that you created, click on it and navigate to horizontal ellipsis and click **Certificate Signing Request**.

16.4 Generate CSR in Bulk

Prerequisites:

- A Space should be assigned to a device. Click **Actions > Assign Space**.
 - If properties of Common-Name, IP Address & DNS Names is selected in the CSR then ensure that they have values in the Device.
1. To create an asset for the template you just created, on the INFER™ UI, navigate to **Inventory > Monitored Assets**.
 2. Click **Register** and select **Multiple Gateways** to register your assets. (or **Single Gateway**, for a single gateway specifically). For more information, see [Registering Things in Bulk](#)
 3. Select the assets that you have created, and click **Actions > Generate CSR**. Note: You can generate a CSR even without selecting an asset. But if you have selected an asset, then ensure that you have selected from the same asset template.
 4. Select the asset template from the drop-down menu, click **Generate**. A Task pop-up appears on the bottom right of UI screen.
 5. Click on the pop-up, and you are directed to the **Task** page.
 6. Once the task is completed, on the Task page, select the task and click on the **Actions > Download**. The CSR is a zip file that gets downloaded on your local machine.

16.5 Signing CSR and Import Certificate

1. On the INFER™ UI, navigate to **Security > Certificates**.
2. Click **Actions**, and select **Sign CSR and Import Certificates**.
3. Select the signed CA Certificate that was uploaded into the INFER™ UI earlier.
4. Click **IMPORT PRIVATE KEY** to import the private key for the CA Certificate.
5. Browse on your local machine for your private key and click **Open**.

6. Under **Private Key Password**, enter the password.
7. Click **IMPORT CERTIFICATE SIGNING REQUESTS** to import the downloaded CSR and click **Import**.

You have now imported and assigned the signed certificates to the assets. Go to Section [Send Command](#).

Note: If you have signed certificates locally, you should import through Import Bulk Certificate.

16.6 Importing Bulk Certificates

This section lists the steps to import signed certificates of the downloaded CSR into INFER™ and assign to device.

Prerequisite: To create a certificate in INFER™, you must have the CREATE_CERTIFICATE permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ UI, go to **Security > Certificates**.
The **Security - Asset Certificates** page appears.
2. Under **ACTIONS** drop-down menu, click **Import Bulk Certificate**.
The **Import Bulk Certificate** pop-up appears.
3. Under **CA Certificate**, select the CA Certificate.
4. Under **UPLOAD CERTIFICATE**, browse to the certificate and click **Upload**.
5. Click **Import**.

You have now imported and assigned the signed certificates to the assets. Go to Section [Send Command](#).

16.6.1 Editing Certificates

This section lists the steps to edit a device certificate in INFER™.

Prerequisite: To create a certificate in INFER™, you must have the EDIT_CERTIFICATE permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ UI, navigate to **Security > Certificates**.
The **Security - Asset Certificates** page appears.
2. Click your desired certificate which requires editing.
3. From the **Actions** drop-down menu, click **Edit**.
The **Update Certificate** pop-up appears.

Note: You can update only the **Name** and **State** fields. Only meta information will be changed in the certificate.

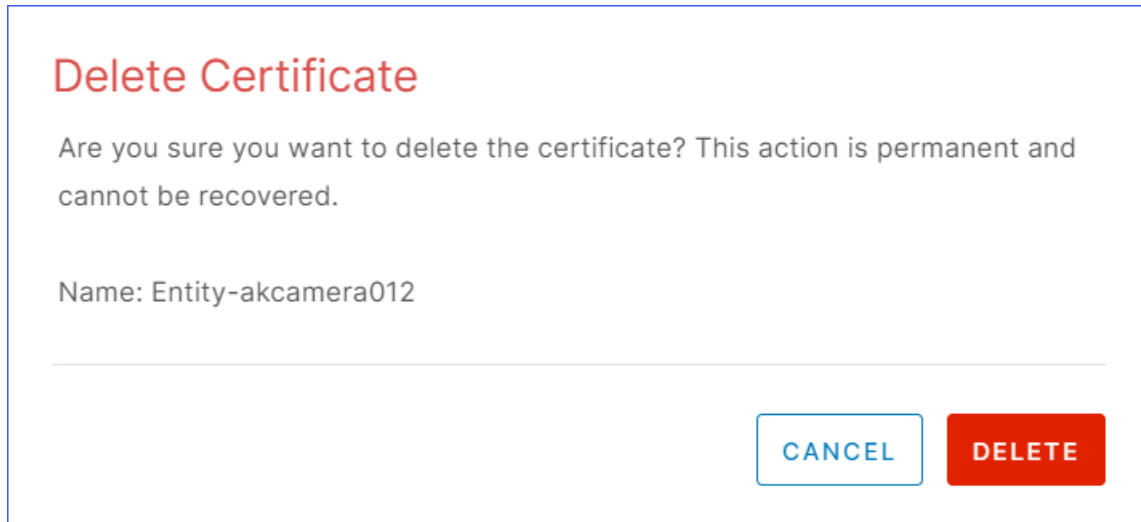
4. After making required changes, click **UPDATE**. The certificate is update and the page defaults to the **Security - Asset Certificates** page listing the updated device certificate.

16.6.2 Deleting Certificates

This section lists the steps to delete a device certificate in INFER™.

Prerequisite: To create a certificate in INFER™, you must have the DELETE_CERTIFICATE permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ UI, navigate to **Security > Certificates**.
The **Security - Asset Certificates** page appears.
2. Click your desired certificate which requires deletion.
3. From the **Actions** drop-down menu, click **Delete**.
The **Asset Certificate** pop-up appears as shown below:



Delete Certificate

Are you sure you want to delete the certificate? This action is permanent and cannot be recovered.

Name: Entity-akcamera012

4. Click **DELETE**. The certificate is deleted from INFER™ and the page defaults to the **Security - Asset Certificates** page.

16.6.3 Assigning Assets

This section lists the steps to assign a device certificate to a device in INFER™.

Note: If you import a certificate manually without CSR generation, then assign asset section is applicable.

Prerequisite: To assign a certificate to a device in INFER™, you must have the CREATE_CERTIFICATE permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ UI, navigate to **Security > Certificates**.
The **Security - Asset Certificates** page appears.
2. Click your certificate which you desire to assign.
3. From the **Actions** drop-down menu, click **Edit**.
The **Assign Asset** pop-up appears.
4. Select the radio button against your desired device as shown below:

Security - Asset Certificates **ACTIONS**

Search across Certificates

Name
Entity-akcamera012
PulseSpSigningCert

1 - 2 of 2 Certificates

Entity-akcamera012 Actions

Basic Information

Name
Entity-akcamera01

Id
7292c042-c339-4 1405

Status
ACTIVE

- Edit
- Delete
- Clone
- Assign Asset**
- Download

- Click **ASSIGN**. The page defaults to the **Security - Asset Certificates** page showing the device certificate assigned under **Assignee Type**.

16.6.4 Unassigning Assets

This section lists the steps to unassign a device certificate from a device in INFER™.

Prerequisite: To unassign a certificate from a device in INFER™, you must have the CREATE_CERTIFICATE permission associated with the Organization Administrator Group, and perform the following steps:

- On the INFER™ UI, navigate to **Security > Certificates**. The **Security - Asset Certificates** page appears.
- Click your certificate which you desire to unassign. The **Unassign Certificate** pop-up appears as shown below:

Unassign Certificate

Are you sure you want to Unassign this certificate?

CANCEL **UNASSIGN**

- Click **UNASSIGN**. The page defaults to the **Security - Device Certificates** page showing the device certificate is not assigned to any device under **Assignee Type**.

16.6.5 Downloading Certificates

This section lists the steps to download a device certificate from INFER™.

Prerequisite: To create a certificate in INFER™, you must have the CREATE_CERTIFICATE permission associated with the Organization Administrator Group, and perform the following steps:

- On the INFER™ UI, navigate to **Security > Certificates**. The **Security - Asset Certificates** page appears.
- Click your certificate which you desire to download.
- From the **Actions** drop-down menu, click **Download**. The certificate is downloaded to your computer.

16.6.6 Send Command

This section lists the steps to send command on INFER™.

1. Once a signed certificate is uploaded into INFER™ using the Import Certificate option, the *upsertCertificate* command should be triggered.
2. On the INFER™ UI, navigate to **Inventory > Monitored Assets**.
The **Inventory - Monitored Assets** page appears.
3. Click on the asset, and click the vertical ellipsis.
4. Click **Command**, click **Send Command**.
5. Select **Set Dot1x**.
6. From the **Command Type**, select *CLIENT_EXECUTE* and click **Send Command**.

17 Working with API Keys

This section describes how to manage your organization's API Keys from INFER™'s **Identity & Access** module.

An API key is a string of characters which serve as a unique identifier to allow access to INFER™. API keys are commonly used to track and manage API usage, restrict access to certain features, and enforce rate limiting.

This module is primarily used by Application Administrators INFER™'s customer organizations who have their enterprise applications in production integrated with INFER™.

They generate API keys or [JW Tokens](#) to establish seamless integration between their enterprise applications and INFER™. An API Key acts as a security token that authorizes the API client to access INFER™.

INFER™ allows you to create, update and revoke an API key. The key can be set to be used for a minimum of 30 days and maximum of 365 days, and can be revoked at any time.

Note: INFER™ sends an email notification to API Key owners 14 days, 7 days, and 1 day before the token's expiration date.

17.1 Key States

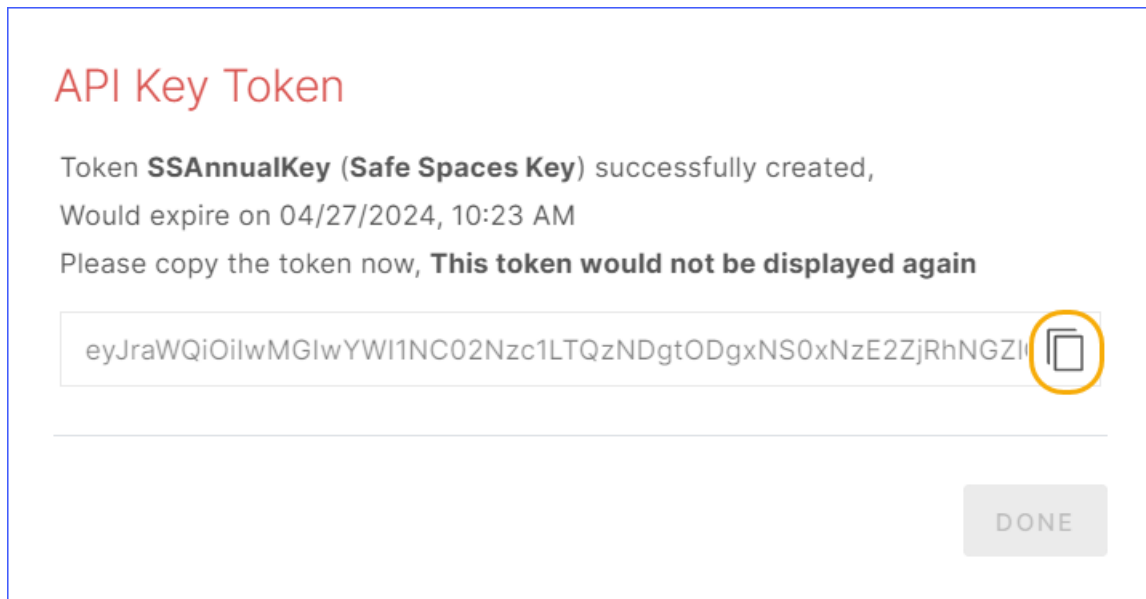
Once created, API Keys pass through the following states:

- Key in active use
- Key disabled by the user
- Key which has outlived its tenure

17.2 Creating a Key

Prerequisite: To create a new API Key in INFER™, you must have the `CREATE_API_KEY` permission associated with the Organization Administrator Group, and perform the following steps:

1. From the INFER™ UI, go to **Identity & Access > API Keys**. The **Identity & Access - API Keys** page appears.
2. Click **CREATE**. The **Create API Key** wizard appears.
3. Under **Display Name** enter the display name of the new key.
4. Under **API Key Name**, enter the name of the new key.
Note: Spaces and special characters are not allowed.
5. Under **Email Address for Notifications**, enter the email address.
6. Under **API Key Validity**, enter a value between 1 to 365 days.
7. Under **Description**, enter a brief description of the new API key and click **NEXT**.
8. Under **Groups / Roles**, under **Groups**, from the **Select Groups** drop-down, select the appropriate groups for this API Key.
9. Next, click the **Roles** tab and from the **Select Roles** drop-down menu, select the appropriate roles for this API Key.
10. Under **Review**, review the information and click **SAVE**. You have successfully created an API key, and the following action confirmation message and **API Key Token** pop-up appears:



11. Click the **Copy to Clipboard** icon to copy the token to the clipboard.
12. Click **DONE**. The page defaults to the **Identity & Access > API Keys** page listing the newly created API Key as shown below:

Token Name	Display Name	Status	Description	Token Expiry (IST)	Token Expiry In Days	Modified (IST)
deviceDiscovery@api.infer.local	Device-Discovery	Expired	This is the api for the device...	10/03/2024, 5:11 PM	-	10/07/2024, 2:35 PM
gpdemo@api.infer.local	gpdemo	Expired	api key to swagger api for Geo...	09/20/2024, 2:24 PM	-	10/07/2024, 2:35 PM
SafeSpacesInc@api.infer.local	SafeSpacesInc	Expired	Production key to interoperate...	04/26/2024, 3:17 PM	-	06/10/2024, 5:58 PM
AgentLessAdapter@api.infer.local	agent-less-adapter	Expired	API key for the agentless adap...	11/26/2023, 10:20 AM	-	03/21/2024, 10:03 AM
ApiCloudAdapters@api.infer.local	API Key for Cloud adapters	Expired	Agentless Cloud adapters	08/09/2023, 4:06 PM	-	10/25/2023, 12:09 PM

Note: Keep API keys secure. Do not share them with unauthorized users, as they can be used to gain access to sensitive data or perform malicious actions.

17.3 Editing a Key

Prerequisite: To edit an API Key in INFER™, you must have the EDIT_API_KEY permission associated with the Organization Administrator Group, and perform the following steps:

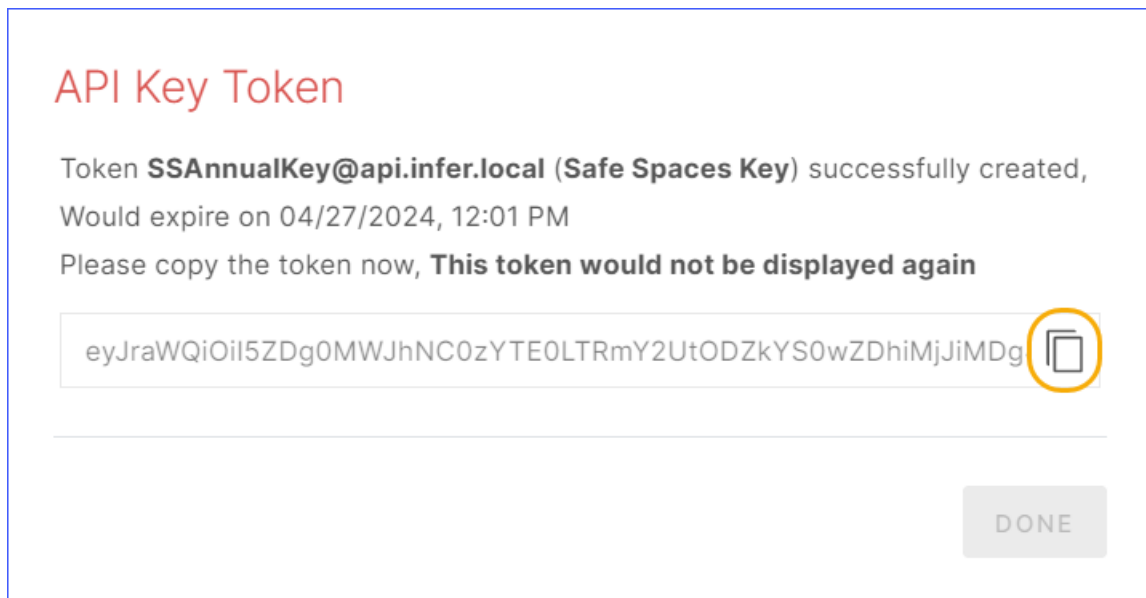
1. On the INFER™ UI, navigate to **Identity & Access > API Keys**. The **Identity & Access - API Keys** page appears.
2. Click the desired key. The details of the key are displayed.
3. From the **Actions** drop-down menu, click **Edit**. The **Edit API Key** wizard appears.
4. Under **Details**, update the display name, api key name, email address, token expiry in days, and description of the key.

5. Click **NEXT**.
6. Under **Review**, review the information and click **SAVE**. You have successfully updated a key.

17.4 Renewing an Key

Prerequisite: To renew an API Key in INFER™, you must have the EDIT_API_KEY permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ UI, navigate to **Identity & Access > API Keys**. The **Identity & Access - API Keys** page appears.
2. Click the desired key. The details of the key are displayed.
3. From the **Actions** drop-down menu, click **Renew**. The **Renew API Key** wizard appears.
4. Under **Details**, you can see that the key details appear non-editable.
5. Under **Review**, review the information and click **RENEW**. You have successfully renewed an API key, and the following **API Key Token** pop-up appears:



5. Click the **Copy to Clipboard** icon as highlighted above to copy the token to the clipboard.
6. Click **DONE**. The page defaults to the **Identity & Access > API Keys** page.

Note: All Key states can be brought to **Renewed** during the following circumstances:

- To ensure uninterrupted business operations, during key creation you can create an extra backup key too.
- Additionally, when the existing key is nearing its expiry date, you can replace it with your backup key before your present key's expiry. In this case, the replaced key gets the **Revoked** status.

17.5 Revoking a Key

Prerequisite: To revoke an API Key in INFER™, you must have the EDIT_API_KEY permission associated with the Organization Administrator Group, and perform the following steps:

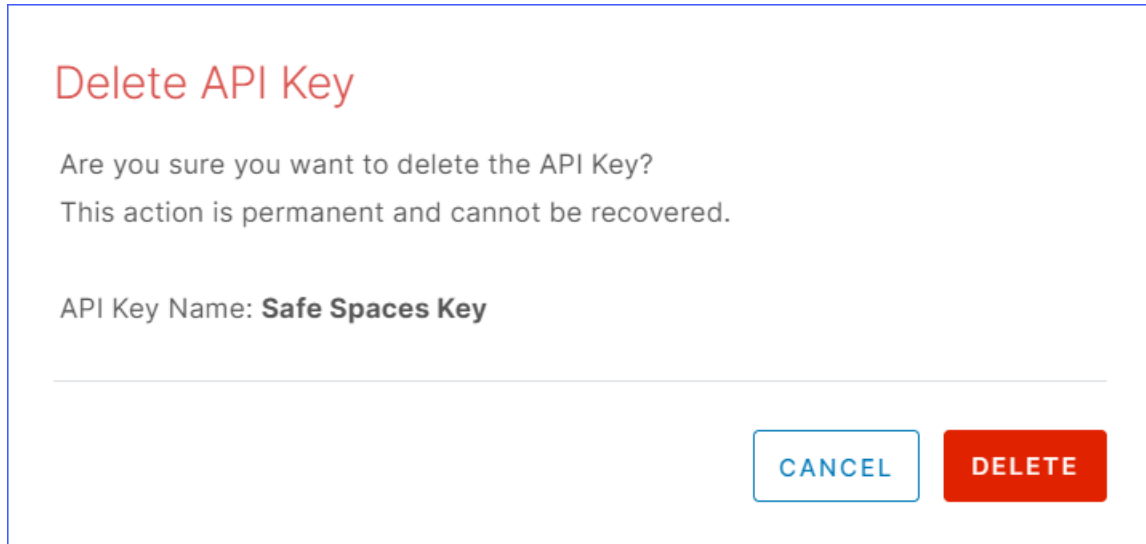
1. On the INFER™ UI, navigate to **Identity & Access > API Keys**. The **Identity & Access - API Keys** page appears.
2. Click the desired key. The details of the key are displayed.
3. From the **Actions** drop-down menu, click **Revoke**. The **Revoke API Key** pop-up appears as shown below:
4. Type **REVOKE** and click **REVOKE**. You have successfully updated a key.
5. The page defaults to the **Identity & Access > API Keys** page displaying the selected API Key's **Revoked** as shown below:

Token Name	Display Name	Status	Description	Token Expiry (IST)	Token Expiry In Days	Modified (IST)
uptimeapicheck@api.infer.local	uptimeapicheck	Active	DO NOT DELETE - Used for uptime...	12/19/2025, 5:21 PM	312 Days	12/19/2024, 5:21 PM
faisaltest@api.infer.local	FaisalTest	Active	To test APIs	08/12/2025, 1:41 PM	183 Days	08/21/2024, 1:41 PM
dstreamerAKey@api.infer.local	DStreamer-API-Key	Active	This API key is being used by ...	06/25/2025, 4:06 PM	135 Days	06/25/2024, 4:06 PM
APIKeyTest@api.infer.local	API Key Test	Revoked	API Key Test	06/14/2024, 2:50 PM	-	04/15/2024, 3:25 PM
prabhuvr@api.infer.local	prabhuvr	Revoked	90	06/08/2024, 12:58 PM	-	03/25/2024, 11:32 AM
TEST20@api.infer.local	Test 20	Revoked	Test 20 Description	10/13/2022, 6:20 AM	-	10/12/2022, 6:21 AM

17.6 Deleting a Key

Prerequisite: To delete an API Key in INFER™, you must have the DELETE_API_KEY permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ UI, navigate to **Identity & Access > API Keys**. The **Identity & Access - API Keys** page appears.
2. Click the desired key. The details of the key are displayed.
3. From the **Actions** drop-down menu, click **Delete**. The **Delete API Key** pop-up appears as below:

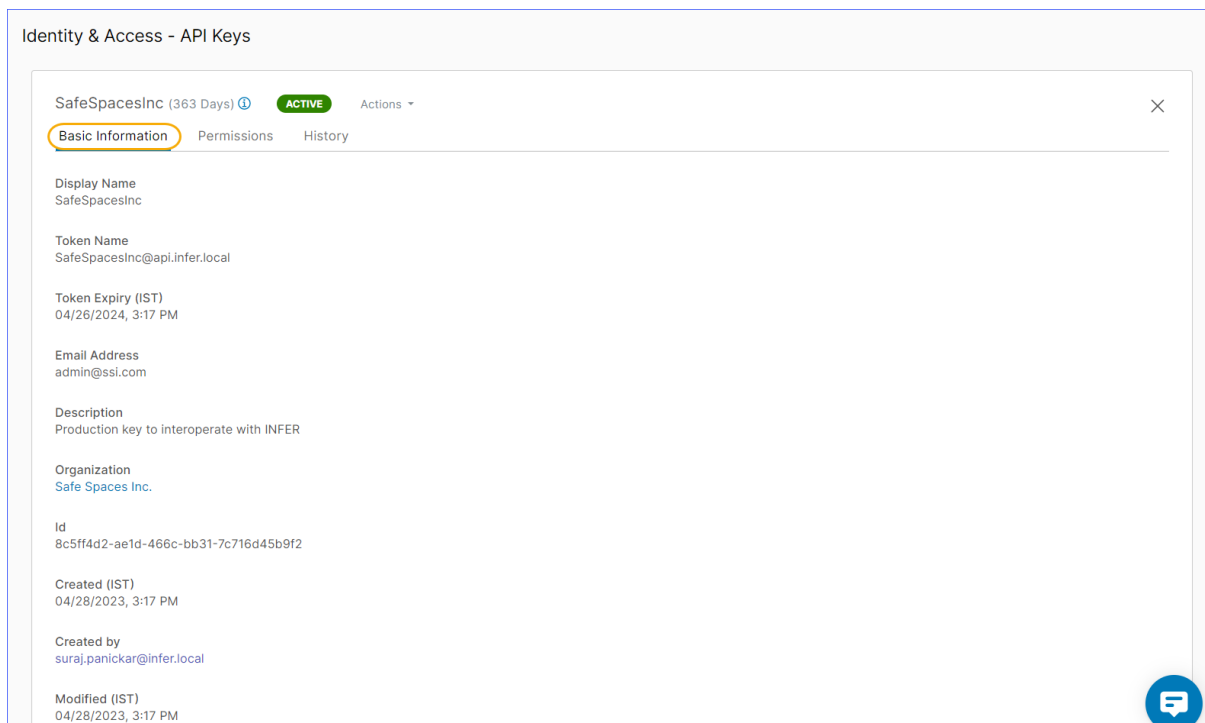


4. Click **DELETE**. You have successfully updated an API key.

17.7 Viewing Key Details

Prerequisite: To view an API Key's details in INFER™, you must have the VIEW_API_KEY permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ UI, navigate to **Identity & Access > API Keys**. The **Identity & Access - API Keys** page appears.
2. Click the desired API key. The details of the key are displayed as shown below:



17.8 Viewing Key Permissions

Prerequisite: To view an API Key's permissions in INFER™, you must have the VIEW_API_KEY permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ UI, navigate to **Identity & Access > API Keys**. The **Identity & Access - API Keys** page appears.
2. Click the desired key.
3. Click **Permissions** tab to view all the permissions associated with this key.
4. Click **EXPAND** to view the complete permissions drill-down.

17.9 Viewing Key History

Prerequisite: To view an API Key's history in INFER™, you must have the VIEW_API_KEY permission associated with the Organization Administrator Group, and perform the following steps:

1. On the INFER™ UI, navigate to **Identity & Access > API Keys**. The **Identity & Access - API Keys** page appears.
2. Click the desired key.
3. Click **History** tab to view the history of this key.

18 Settings

The **Settings** module allows users to configure and customize various settings according to the specific needs and requirements of their organization.

You can define organization settings at the root level so that the settings are applied to all the sub-organizations under the root organization. This way, you need not apply settings individually to all sub-organizations under an organization. The sub-organizations can either use the applied settings or override them.

Prerequisite: To view and edit the parameters listed below, you must have the VIEW_ORGANIZATION_SETTINGS and EDIT_ORGANIZATION_SETTINGS permissions associated with the Organization Administrator Group.

18.1 Setting up Custom Branding

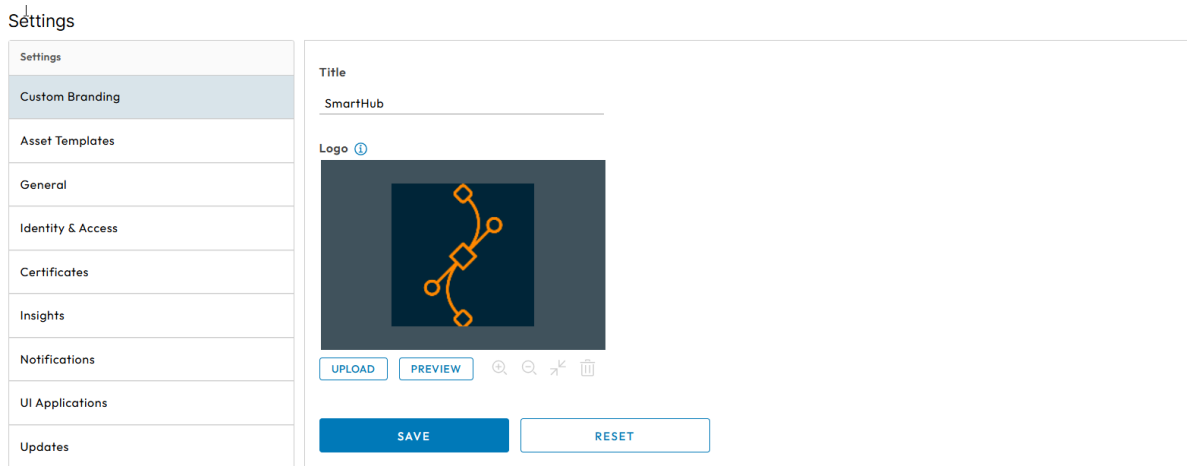
Consistency in branding across all touch-points helps create a cohesive and memorable brand experience for your customers.

The Custom Branding module is a powerful tool to customize the visual identity and appearance of to align with your organization's broader brand identity.

The Settings module helps to promote your organization's brand recognition, building trust with your customers, and highlight the values and personality of your organization's brand.

To create a new custom brand in INFER™, perform the following steps:

1. On the INFER™ UI, navigate to **Settings**. The **Custom Branding** tab appears selected by default as shown below:



The screenshot displays the 'Settings' page in the INFER™ UI. On the left, a sidebar contains a list of settings categories: Settings, Custom Branding (highlighted), Asset Templates, General, Identity & Access, Certificates, Insights, Notifications, UI Applications, and Updates. The main content area is titled 'Custom Branding' and includes a 'Title' field with the text 'SmartHub'. Below this is a 'Logo' field with a placeholder image of a network diagram. Under the logo are three buttons: 'UPLOAD', 'PREVIEW', and 'SAVE'. At the bottom of the main area are two buttons: 'SAVE' and 'RESET'.

2. Under **Title**, enter your organization's name.
3. Under **Logo**, drag and drop or upload an image with file size lesser than 500KB.
4. Click **UPLOAD**.
5. Click **PREVIEW** to verify the title and uploaded logo.
6. Click **SAVE**. You have successfully created your custom branding.
7. Click **RESET** to revert to default settings.

18.2 Setting up the Default Gateway & Thing Template

The Settings module in allows you to define the default set of System and Custom properties for gateways and thing devices onboarded for the Organization.

To define the default set of System and Custom properties in INFER™, perform the following steps:

1. On the INFER™ UI, navigate to **Settings > Asset Templates**. This tab appears as shown below:

Settings

- Settings
- Custom Branding
- Asset Templates**
- General
- Identity & Access
- Certificates
- Insights
- Notifications
- UI Applications
- Updates

The Default Set of System & Custom properties for this Organization

Default Gateway Template

Default Gateway Template

or

IMPORT

COPY

```
{
  "id": "ed2c70d5-c7af-4eb1-a9b1-f64bd454d5e",
  "name": "Default Gateway Template",
  "tenantId": "aeede24d-2d79-49b8-af1d-ffc06b2a61d5",
  "deviceType": "GATEWAY",
  "systemProperties": [
    {
      "name": "os updates-reboot required",
      "description": "If reboot is required after the update",
      "value": "-"
    },
    {
      "name": "os updates-pending-total",
      "description": "Total number of pending os updates",
      "value": "10"
    },
    {
      "name": "os updates-pending-security",
      "description": "Number of os security updates pending",
      "value": "-"
    }
  ]
}
```

SAVE RESET

Default Thing Template

Select Asset Template

or

IMPORT

COPY

```
{
  "name": "Default Thing Template",
  "deviceType": "THING",
  "customProperties": [
    {
      "name": "Application-ApplicationNameList",
      "value": "-"
    },
    {
      "name": "Asset-Identity-ID",
      "value": "-"
    }
  ]
}
```

2. Under **Default Gateway Template** drop-down menu, select a default template. The selected template's JSON code appears in the text area as highlighted above.
3. Alternately, click **IMPORT** to upload a JSON template file. The uploaded JSON file's content appears in the text area below.
4. Click **COPY** to copy the code to the clipboard and review/modify the same in an external code editor.
5. Next, under **Default Thing Template**, use the drop-down to select the default template. The selected template's JSON code appears in the text area below.
6. Alternately, click **IMPORT** to upload a JSON template file. The uploaded JSON file's content appears in the text area below.
7. Click **COPY** to copy the code to the clipboard and review/modify the same in an external code editor.
8. Click **SAVE**.
9. Click **RESET** to revert to default settings.

18.3 Setting up Audit Log Retention Period

The Settings module allows you to define the audit log retention period for the organization.

The audit log retention period, also known as data retention policy for audit logs, refers to the duration for which your organization keeps records of audit logs and related activity data. The appropriate audit log retention period varies based on factors like regulatory requirements, organizational policies, and security considerations.

Audit logs contain a chronological record of events, actions, and transactions within. These logs are critical for security, compliance, and troubleshooting purposes.

To define the audit log retention period for the organization in INFER™, perform the following steps:

1. On the INFER™ UI, navigate to **Settings > General**. This tab appears as shown below:

Settings

Settings
Custom Branding
Asset Templates
General
Identity & Access
Certificates
Insights
Notifications
UI Applications
Updates

Audit log retention period

30 Days

API Key Maximum Validity

365 Days

SAVE **RESET**

2. Under **Audit log retention period**, specify the number of days.
3. Enter **API Key Maximum Validity** days.
4. Click **SAVE**.
5. Click **RESET** to revert to default settings.

18.4 Setting up Identity & Access

The Settings module in INFER™ allows you to configure external identity provider (IdP) to authenticate access to the INFER™ platform.

INFER™ uses IdPs as a third-party service to manage and authenticate user identities and provide Single Sign-On (SSO) capabilities.

18.4.1 Setting up SAML Authentication

Security Assertion Markup Language (SAML) single sign-on (SSO) uses third-party authentication service providers to provide access to users.

SAML SSO works by transferring the user's identity from the identity provider (IdP) to the authentication service provider, through the exchange of digitally signed XML metadata.

To configure the SAML SSO settings for your organization, perform the following steps:

1. On the INFER™ UI, navigate to **Settings > Identity & Access**.
2. The **Enable external Identity Provider** switches ON by default.
3. Under **IDP Type**, **SAML** option in the drop-down menu appears selected by default.
4. The **Just In Time user creation** switch appears ON by default, and allows all valid IdP users to login. To disable **Just In Time user creation**, click to switch OFF.

Note:

- With this option enabled, INFER™ creates a shadow user if the user does not exist in any of the organizations.
- If you disable this option, the user cannot access INFER™ even though the user credentials are configured in the external IdP.
- All valid IdP users can log in to INFER™ when this option is enabled.
- To disable Just In Time (JIT) user creation, deselect Enable JIT user creation.

- If you decide to update the Just In Time user creation settings at a later stage, you must reconfigure the SAML settings.
5. Under **SAML Settings > Step 1: SAML Certificates > Signing Key**, click **Choose File** and select the custom certificate from your local folder. This certificate is used as a signing key to access metadata.
Note: If you do not provide a certificate, INFER™ generates a self-signed certificate. To skip this step, click **NEXT**.
 6. Under **Signing Key Password**, if the certificate is password protected, enter the password to access it.
 7. Under **Encryption Key**, click **Choose File** and select the encryption key for the certificate.
 8. Under **Encryption Key Password**, enter the password for the encryption key.
 9. Click **UPDATE CERTIFICATE**.
 10. Next, under **Step 2: Service Provider Metadata Download**, click **DOWNLOAD** to download the Service Provider (INFER™) metadata and copy the content. Alternately, you can copy the metadata content from the **SAML Service Provider Metadata** text box also.
 11. Under **Step 3: Identity Provider Setup**, navigate to your Identity Provider administrator page and configure INFER™ as a Service Provider. Copy the downloaded service provider metadata to a text file and save it with the `.xml` extension. For example, `INFERSP_metadata.xml`. Use the saved service provider (SP) metadata to configure the service provider settings on the IDP. To authenticate the user, you must assign the user to the IDP. This authenticates the user to log in to for the particular organization.
Note: In the organizational structure, a user has access rights that are designed to reflect their level in the hierarchy (sub-organizations). Users with a higher-level access to an organization or even a sub-organization will also have access to all the sub-organizations within that organization. To set the SAML SSO authentication for your user on multiple sub-organizations, you must register the service provider in the IDP for each of the sub-organizations. Use the sub-organization's SP metadata to register.
 12. Under **Step 4: Saml Setup > SAML Authentication URL**, enter the external IdP's authentication URL to which you post the request to INFER™.
Note: In the INFER™, user roles and permissions are determined dynamically based on Active Directory (AD) grouping. When users log in through the Identity Provider (IDP) via Single Sign-On (SSO), INFER™ automatically assigns the appropriate roles and permissions. The system maps users to groups and assigns permissions on the fly, ensuring they have the necessary access to perform their designated tasks efficiently. This seamless integration between the IDP and INFER™ streamlines access management and ensures that permissions align with users' responsibilities.
 13. Under **SAML Metadata XML**, enter the URL or the metadata of the external IdP. You can access the metadata by sending a GET request to the external IdP, or copy the same from the text area below.
 14. Under **Attribute Mapping**, you can add and map IDP Attribute keys into INFER™.
 - Click the **Edit** icon to edit the attribute keys for creating the user, and click **DONE**.
 - Click the **+ Add** icon to add a new attribute keys for creating the user.
 - Click the **Delete** icon to delete an existing key.

Note: **userName**, **email**, and **displayName** are mandatory keys. These keys must be mapped to the **UserName**, **DisplayName**, and **Email** keys in the IdP.

15. Next, under **Group Mapping**, you can add and map IDP Group keys into INFER™.

- Click the **Edit** icon to edit the group details of the user.
- Click the **Delete** icon to delete an existing group.
- To add a new group for creating the user, click **+ Add** icon.
- Under **Group Name**, enter the new group name.
- Next, under **Infer Group Name** select the desired groups from the drop-down menu and click **DONE**.

16. Click **SAVE**. You have successfully configured the SAML SSO authentication settings in INFER™.

17. Click **RESET** to revert to default settings.

18.4.2 Setting up LDAP Authentication

LDAP (Lightweight Directory Access Protocol) authentication is a method used to verify the identity of users or devices attempting to access a system or network resource by querying a directory service, typically a LDAP Server. LDAP is commonly used for authentication and authorization in various enterprise networks, web applications, and email services.

To configure the Lightweight Directory Access Protocol (LDAP) settings for your organization, perform the following steps:

Note:

- INFER™ is integrated with LDAP.
- LDAP is supported on on-premise versions of INFER™.

1. On the INFER™ UI, navigate to **Settings > Identity & Access**.

2. The **Enable external Identity Provider** switch appears ON by default.

3. Under **IDP Type**, select **LDAP** from the drop-down menu.

4. The **Just In Time user creation** switch appears ON by default, and allows all valid IdP users to login.

Note:

- With this option enabled, INFER™ creates a shadow user if the user does not exist in any of the organizations.
- If you disable this option, the user cannot access INFER™ even though the user credentials are configured in the external IdP.
- All valid IdP users can log in to INFER™ when this option is enabled.
- To disable Just In Time (JIT) user creation, deselect **Enable JIT user creation**.
- If you decide to update the **Just In Time user creation** settings at a later stage, you must reconfigure the SAML settings.

5. Under **LDAP Settings > Domain Name** text box, enter a valid domain name.
6. Under **Server Details > Directory Type**, select the directory type.
7. Under **Host**, enter a valid host IP address.
8. Under **Port**, enter the port number.
9. Under **Authentication Type**, select the desired authentication type.
10. Under **Encryption Type**, select the desired encryption type.
11. Under **User Details > Bind Username**, enter the BIND user name.
12. Under **Bind Password**, enter the BIND password.
13. Under **User Object Class**, enter the object class associated with the user.
14. Click **TEST CONNECTION** to ensure that the connection is successful.
15. Click **SAVE**. You have successfully configured the LDAP authentication settings in INFER™.
16. Click **RESET** to revert to default settings.

You can now log in to Console with the external IdP credentials.

18.5 Setting up Insights Dashboard

The **Insights** module offers you a pre-configured, out-of-the-box dashboard that gives you a starting point for data exploration and analysis without building a dashboard from scratch. These default dashboards include common key performance indicators (KPIs), visualizations, and reports that are relevant to you.

To configure the default Insights dashboard in INFER™, perform the following steps:

1. On the INFER™ UI, navigate to **Settings > Insights**. This tab appears as shown below:

Settings

Settings
Custom Branding
Asset Templates
General
Identity & Access
Certificates
Insights
Notifications
UI Applications
Updates

Default dashboard link

d/ivKh/CDVKH/executive-summary?orgId=1

SAVE **RESET**

2. Under **Default dashboard link**, enter the link to your organization's dashboard as highlighted above.
3. Click **SAVE**. You have successfully configured the default dashboards settings in INFER™.
4. Click **RESET** to revert to default settings.

18.6 Setting up Notification Retention Period

The notification retention period refers to the duration for which notifications, alerts, or messages are stored and accessible by you before they are automatically deleted or archived.

To update the notification retention period for your organization and all its sub-organizations, perform the following steps:

1. On the INFER™ UI, navigate to **Settings > Notifications > Notification**. This tab appears as shown below:

Settings

Settings
Custom Branding
Asset Templates
General
Identity & Access
Certificates
Insights
Notifications
UI Applications
Updates

Notification Notification Definitions System Notifications

Notification retention period

30 Days

SAVE **RESET**

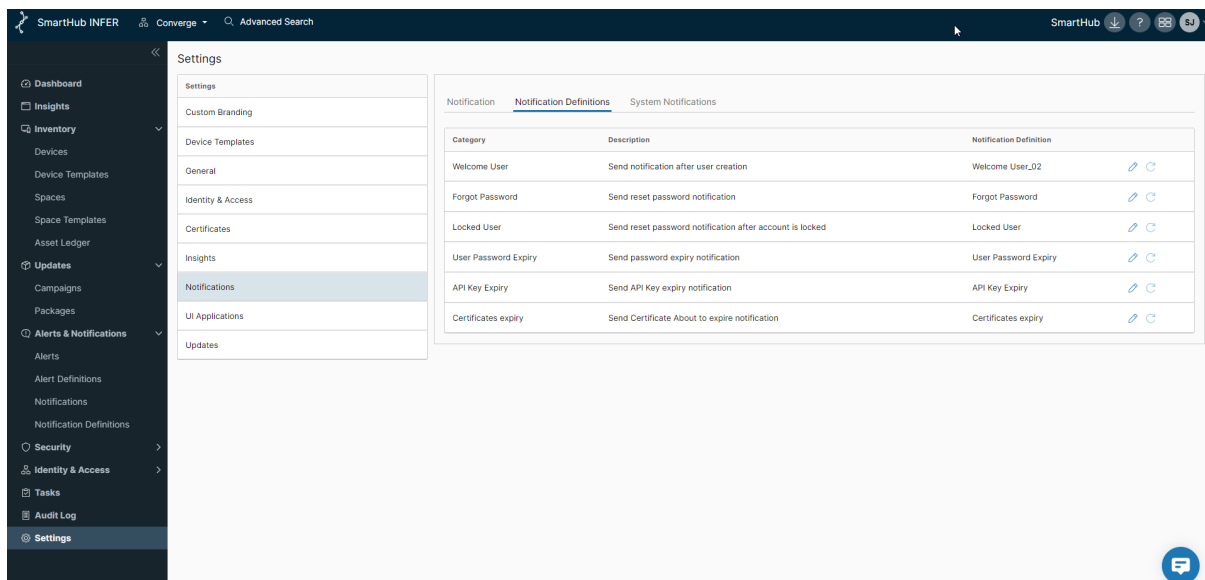
2. Under **Notification retention period**, specify the number of days.
Note: The default notification retention period is 30 days.
3. Click **SAVE**. You have successfully set the notification retention period for your organization in INFER™.
4. Click **RESET** to revert to default settings.

18.7 Setting up Notification Definitions

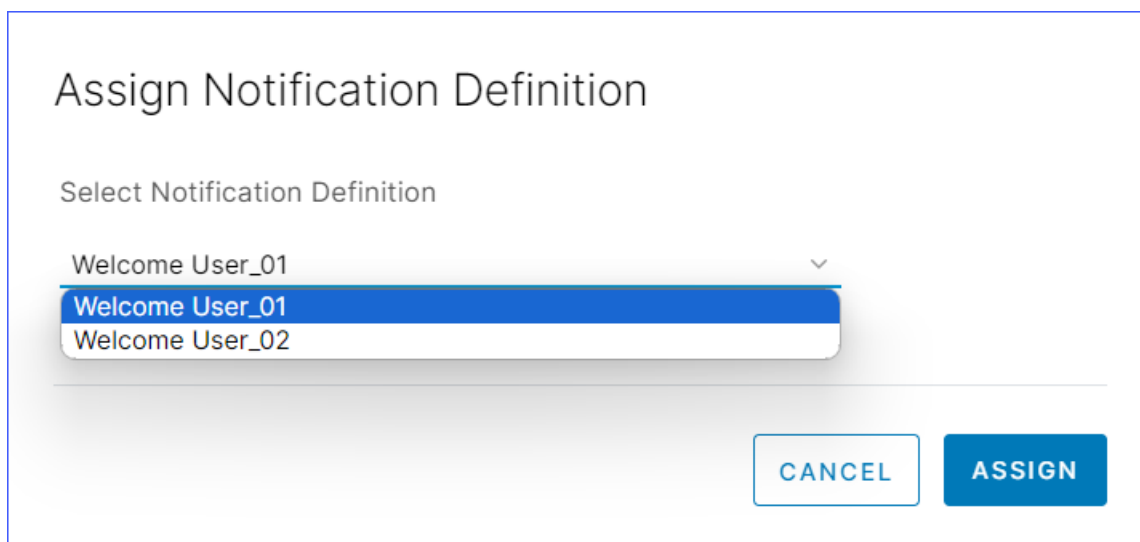
Notifications in INFER™ are email and REST-based alerts that inform users or other parts of a system about important events, updates, or changes. For more information on notification definitions, see [What is a Notification Definition?](#).

To edit the default notification definitions for your organization and all its sub-organizations, perform the following steps:

1. On the INFER™ UI, navigate to **Settings > Notifications > Notification Definitions**. The default list of notification definitions appears as shown below:



2. Under **Category**, click the **Edit** icon to assign notification definitions. The following pop-up appears as shown below:



3. Select the desired definition from the drop-down menu.
4. Click **ASSIGN**. The default notification category is updated.

18.8 System Notifications Settings

System notifications are automated email messages generated based on predefined triggers or events to inform user groups, users, or email addresses of your organization about important events or updates in .

To send system notification emails to users belonging to a particular group, listed users, or email addresses, perform the following steps:

1. On the INFER™ UI, navigate to **Settings > Notifications > System Notifications**. This tab appears as shown below:

Settings

- Settings
- Custom Branding
- Asset Templates
- General
- Identity & Access
- Certificates
- Insights
- Notifications**
- UI Applications
- Updates

Notification Notification Definitions **System Notifications**

Send System Notification Emails to users belonging the following groups, listed users or email addresses.

Groups

Select Group ▾

Group Name	
Organization Administrators	🗑️
System Administrators	🗑️

Users

Add User ▾

Email

Recipients
+Add Recipient

SAVE **RESET**

2. Under **Groups**, click **Select Group** drop-down menu to select the required groups.
3. Under **Users**, add email IDs from the drop-down menu.
4. Under **Email**, add the recipient's email ID, and click **DONE**.
5. Click the **+ Add** icon to add another recipient.
6. Click **SAVE**. You have successfully created system notifications settings for your organization in INFER™.

18.9 UI Applications

If you have a vertical solution from SmartHub INFER™, then you can choose a default UI application as your default login when you log into your organization. The default UI will be associated with a current organization. Users of sub-org will have access to the selected org only and its sub-orgs.

1. Under the **UI Applications** tab, click on any of the tabs on the screen.
2. Click **SAVE**.


Settings

Settings
Custom Branding
Asset Templates
General
Identity & Access
Certificates
Insights
Notifications
UI Applications
Updates


Default UI Application

Choose the default application to be launched on login for the current organization.


☐ You do not have permission to set the Default application, contact system administrator.



INFER



CONVERGE



AQUA

SAVE

18.10 Setting up OTA Updates

Over The Air (OTA) updates eliminate the need for manual downloads, making it easy for users to keep their devices up-to-date.

To enable approvals for the OTA updates that are run in your sub-organizations, perform the following steps.

1. On the INFER™ UI, navigate to **Settings > Updates**. This tab appears as shown below:

Settings

Settings
Custom Branding
Asset Templates
General
Identity & Access
Certificates
Insights
Notifications
UI Applications
Updates

☒ Enable Approvals

Toggle the Enable Approvals button to add an approval step in your campaign workflow. By enabling approvals, your campaign requires an approval from a user having the Approve Campaign* permission before it starts.

SAVE RESET

2. Toggle **Enable Approvals** option to switch ON approvals for all OTA updates that your sub-organizations runs.
3. Click **SAVE**. You have successfully enabled approvals for OTA updates for your organization in INFER™.
4. Click **RESET** to revert to default settings.

19 Troubleshooting

If you encounter problems while using INFER™, you can use a troubleshooting topic to understand and solve the problem, if there is a workaround.

19.1 Troubleshooting Campaign Management

You can find troubleshooting steps for common campaign management problems in this section.

19.1.1 Prerequisites

To monitor the progress of a campaign on the gateway, set the `agentLogLevel` to 6 in the `iotc-agent.cfg` file. You can then monitor the system logs to view the progress of the campaign using tools such as `journalctl -u iotc-agent -f`.

19.1.2 The INFER™ Agent Fails to Run with the "Exec Format Error" Message

Workaround:

- Prefix the script with a shebang (`#!`).
- If you are running an executable, run it in a standalone staging environment without the INFER™ Agent. If the executable fails, fix the executable and try again. If the executable runs successfully, contact SmartHub Support.

19.1.3 Package Manifest File - the Packages Are Not Downloaded, Activated, or Executed

Workaround:

- Ensure that your package is being executed in the `headless` mode.
- Ensure that the `manifestExecution` property is enabled in the `iotc-agent.cfg` file.

19.1.4 Agent SDK - the Packages Are Not Downloaded, Activated, or Executed

Workaround:

- Ensure that the respective lifecycle phase is scheduled with the `defaultClient` or the API.
- Ensure that the `manifestExecution` property is disabled in the `iotc-agent.cfg` file.

19.2 INFER™ Agent Connectivity to the INFER™ Server

When you onboard a gateway, at times, the assets are unable to connect to INFER™ Center and an error message appears. The syslog messages indicate that there is a connectivity problem.

You must perform the following checks:

1. Verify if the INFER™ instance is reachable from the gateway.

1. Verify the following log location: `/var/log/syslog` or `/var/log/messages` or `journalctl`. If you see the following error in the log file on the gateway asset:
`Curl_easy_perform() failed : Could not connect to server.`

2. Verify the INFER™ Server. Run the following command:

```
Curl -v https://<INFER-server>`Ping <INFER-server>
```

2. Verify the INFER™ agent logs for connection errors.

1. Verify the log location on the gateway asset: `/var/log/syslog` or `/var/log/messages` or `journalctl`

3. After enrolling, if there is no communication between the INFER™ agent and the INFER™ Server, verify the INFER™ agent logs for token errors in the location : `/var/log/syslog` or `/var/log/messages` or `journalctl`

The following error message appears in the log file on the gateway asset:

```
ERROR: GetCommand: HTTP GetCommand Request failed: ["Invalid Device token"]
```

4. If the preceding step fails, contact SmartHub Support.

Note: If historical data associated with the gateway is not important, then you can try re-enrolling the gateway asset. See [Onboarding Gateways](#).

19.3 Frequently asked Questions

1. Why is a campaign stuck in an Initialized State?

Answer - One of the possible reason is agent is not running on the gateway or the connectivity of the agent with INFER™ is lost. To confirm that agent is up and running, and the connectivity with INFER™ is fine check if the Gateway metric is streaming into INFER™.

2. Why is the password under System properties and Custom Properties not encrypted?

Answer - Ensure the password field is set as Sensitive at the Asset Template level. Once the properties are set as sensitive at the template level it should propagate to the asset properties.

3. I have multiple assets enrolled on my Gateway. How can I identify which assets need a firmware update and find the latest firmware version number? How can I track which assets require an update?

Answer: Go to the Insights dashboard on the INFER™ UI. The Firmware Summary will display the age of your camera firmware and its support expiry details. **Note:** It is recommended not to have more than 100 assets connected to a gateway.

20 Integrating with Third-Party CMS

To perform over-the-air software updates, operating system updates, and firmware updates to the gateways and assets managed by INFER™ using a third-party content management system (CMS), integrate the third-party CMS with INFER™.

You must be a INFER™ administrator to perform this operation.

If you use an external CMS to store software, firmware, or operating system updates for your gateways and assets, use the **uploadProgram** API to integrate the CMS with INFER™.

For more information, see the [INFER™ API Reference Guide](#).

21 TPM-Based Attestation

TPM-based attestation is a process to detect gateway tampering for file systems.

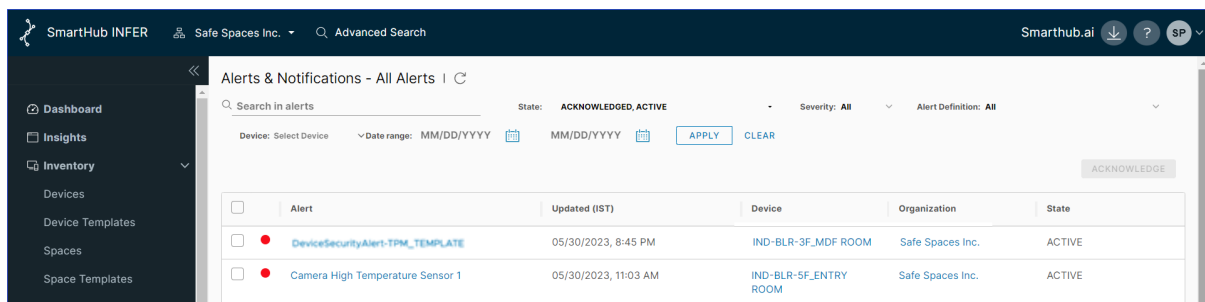
With the TPM-based attestation configured, INFER™ triggers an alert whenever a gateway is tampered.

TPM-based attestation are of two types:

- Boot Attestation
- Runtime Attestation

21.1 What is Boot Attestation?

Boot attestation is a secure mechanism to verify the integrity of an IoT gateway during boot time. Boot attestation enables the detection of gateway file tampering every time the gateway boots. When a tampering is detected, INFER™ raises an alert.

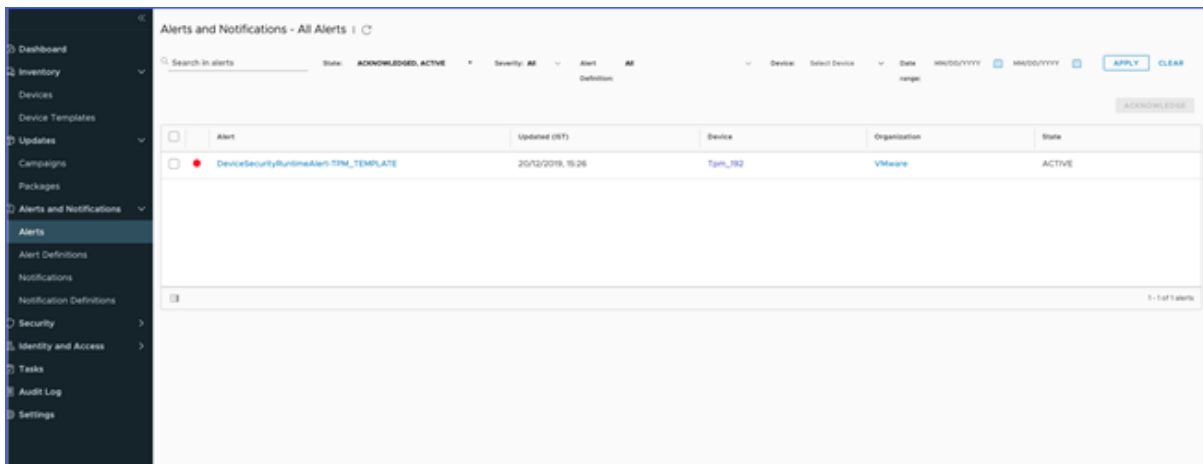


The cause of failure is updated in the gateway properties.

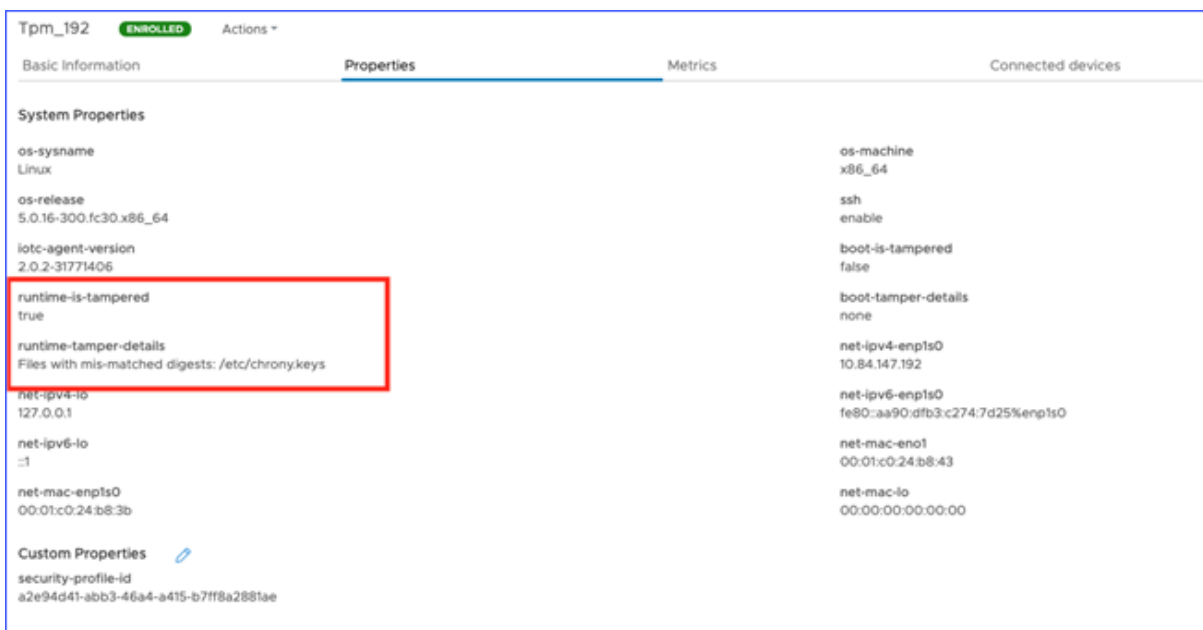


21.2 What is Runtime Attestation?

Runtime attestation is a secure mechanism to verify the integrity of an IoT gateway during run time. The runtime attestation check occurs every 3600 seconds. When a tampering is detected, INFER™ raises an alert.



The cause of failure is updated in the device properties.



Note: Runtime attestation is supported on Fedora IoT operating systems running on CompuLab IoT gateways.

To configure the runtime attestation, you must enable Integrity Measurement Architecture (IMA) on your gateway.

21.3 What Is Integrity Measurement Architecture?

Integrity Measurement Architecture (IMA) is an open source trusted computing component.

IMA, when anchored in a hardware Trusted Platform Module (TPM), maintains a runtime measurement list with an aggregate integrity value of the list. This ensures that the measurement cannot be tampered without it being detected. Hence, on a trusted-boot system, the IMA can be used to attest to the system's runtime integrity.

21.4 Preparing Your Gateway for Boot Attestation

To prepare your gateway for boot attestation, you must generate a fingerprint.json file.

1. To generate a fingerprint, run the following command:

```
/opt/smarthub/iotc-agent/bin/fingerprint dev \> fp.json
```

A fingerprint file `fp.json` is generated.

2. Verify the fingerprint file:

```
cat fp.json
```

3. Using the `fp.json` file, you can now create a boot attestation profile from the INFER™ Console.

21.5 Preparing Your Gateway for Runtime Attestation

For INFER™ to detect tampering, you must configure the following IMA settings on your gateway.

21.5.1 Configuring the Kernel

Append the Kernel command line with the following flag:

```
rootflags=i_version ima_policy=tcb ima_hash=sha256
```

For example, on a Fedora Workstation:

1. Edit `/etc/default/grub` with:

```
`GRUB_CMDLINE_LINUX=\`" rootflags=i_version ima_policy=tcbima_policy=secure_boot
↪ ima_hash=sha256\`"
```

```
`Bash
```

2. ``sudo grub2-mkconfig -o /boot/efi/EFI/fedora/grub.cfg``.

****Note**:** These steps might not work with a Fedora IoT image. Perform the following steps if the preceding steps do not work:

1. Open the ``/boot/loader/entries/ostree-1-fedora-iot.conf`` file and add the following flag to the line that starts with ``options``:

```
`"rootflags=i_version ima_policy=tcb ima_hash=sha256\`"
```

2. Restart the gateway for the settings to take effect.

Modifying the `/etc/fstab` File

Add the following line to the ``fstab`` file:

```
`UUID=d4bbe97d-a719-43af-a89a-19a9455cec5b / ext4 noatime,iversion 1 1`
```

Obtaining the Golden Values for Runtime Attestation

For the runtime attestation to work, you must record the current good state of your gateway. For this, you must run the ``ima_snapshot`` tool on the gateway.

1. To generate ``ima-policy``, run the following script:

```
`/opt/smarthub/iotc-agent/script/install-ima-policy.sh`
```

The ``ima-policy`` is generated and is placed in ``/etc/ima/ima-policy``.

2. To generate ``ima-snapshot` file`, run the following script:

```
`/opt/smarthub/iotc-agent/bin/ima_snapshot -o <<ima.json
path>>`
```

****Note:****

- Add all the paths to be excluded in a file and provide the file path to ``-e`` option in the final ``ima-snapshot`` file.
- Edit the ``ima-snapshot` file` and delete all the ``/usr/lib` and `/usr/lib64`` `file` paths.

3. Verify the file by running the following command:

```
`cat ima.json`
```

****Note:**** The ``ima.json` file` must contain all the hashes.

4. Generate a fingerprint file. Run the following command:

```
`/opt/smarthub/iotc-agent/bin/fingerprint dev \> fp.json`
```

5. Verify the ``fingerprint`` file:

```
`cat fp.json`
```

Using the ``ima-snapshot`` and ``fp.json`` files, you can now create a runtime attestation profile from the INFER™ Console.

Creating a Boot Attestation Profile

Use the ``fp.json` file` to create a boot attestation profile in the INFER™ Console.

****Prerequisite**:** You must have created a TPM-based device template. The `TPM-based` template contains the following system properties:

- runtime-tamper-details
- boot-tamper-details
- runtime-is-tampered
- boot-is-tampered

The template also contains the following custom property:

- ****security-profile-id****

1. On the INFER™ UI, navigate to ****Security**** `\>` ****Profiles****.

2. Click ****ADD PROFILE****.
The ****Add Profile**** wizard appears.

3. In the ****Details**** step:

1. Enter a profile name.

2. In the **Asset Template** drop-down menu, select the TPM-based device template that you have created.
3. Under **Notes**, enter information about the profile.
4. Click **NEXT**.
4. In the **Boot Attestation** step, click **UPLOAD** and upload the `fp.json` file. Click **NEXT**.
5. In the **Runtime Attestation** step, click **NEXT**.
6. In the **Review** step, review the updates and click **SAVE**.

You have successfully created a boot attestation profile. You can view your profile under **Security** > **Profiles**.

An alert definition is created for this profile. The alert definition is used for generating alerts when your gateway is tampered. To view the alert definition, go to **Alerts & Notifications** > **Alert Definitions**.

Next, you can associate this profile with the TPM-based template.

Creating a Runtime Attestation Profile

Use the `ima-snapshot` and `fp.json` files to create a runtime attestation profile in the INFER™ Console.

Prerequisite: You must have created a TPM-based asset template. The TPM-based template contains the following system properties:

- runtime-tamper-details
- boot-tamper-details
- runtime-is-tampered
- boot-is-tampered

The template also contains the following custom property:

- **security-profile-id**

1. On the INFER™ UI, navigate to **Security** > **Profiles**.
2. Click **ADD PROFILE**.

The Add Profile wizard appears.

3. In the **Details** step:
 1. Enter a profile name.
 2. In the **Asset Template** drop-down menu, select the TPM-based asset template that you have created.
 3. Under **Notes**, enter information about the profile.

4. Click **NEXT**.

4. In the **Boot Attestation** step, click **UPLOAD** and upload the `fp.json` file. Click **NEXT**.
5. In the **Runtime Attestation** step, click **UPLOAD** and upload the `ima.json` file. Click **NEXT**.

Note: The maximum size allowed for uploading is 20 MB.

6. Under **Review**, review the updates and click **SAVE**. You have successfully created a runtime attestation profile. You can view your profile under **Security** > **Profiles**.

An alert definition is created for this profile. The alert definition is used for generating alerts when your gateway is tampered. To view the alert definition, go to **Alerts & Notifications** > **Alert Definitions**.

Associating the Attestation Profile with TPM-based Template

After creating an attestation profile, you must associate it with the TPM-based template. This ensures that the gateways you enroll using the TPM-based template are tamper-detectable.

Prerequisite: You must have a valid attestation profile.

1. On the INFER™ UI, navigate to **Security** > **Profiles**.
2. Copy the Profile ID of the attestation profile that you have created.
3. Go to **Asset Templates** and click the TPM-based template that you have created.
4. Scroll down to the **Custom Properties** section and click the edit icon.
5. In the **Edit Custom Property** window, click the edit icon against the security-profile-id.
6. Paste the Profile ID under the **Default Value** text box. Click **DONE**.
7. Click **SAVE** to save the changes.
8. Next, configure the TPM attestation level in your gateway. Run the following command to open the `iotc.cfg` file:

```
`vi /opt/smarthub/iotc-agent/conf/iotc-agent.cfg`
```

9. Set the TPM attestation level to full:

```
`tpmAttestationLevel = full`
```

Note:

- If you want to enable only boot attestation, then set `tpmAttestationLevel = boot`

- If you want to enable both runtime and boot attestation, set
↪ ``tpmAttestationLevel = full``

You have successfully associated the attestation profile to your TPM-based asset template. You can now onboard your gateway using the TPM-based template.

Next, onboard a gateway using the TPM-based authentication method. For [more](#) information, see ****[Onboarding a Gateway using TPM-based Authentication]****.

After on-boarding your gateway, go to ****Audit Log**** in the INFER™ Console and verify that the following audit types are displayed:

- ****TPM Boot Attestation Succeeded****
- ****Runtime Boot Attestation Succeeded****

If there is an attestation failure, verify the following:

- Verify the ****Alerts**** tab for any alerts corresponding to the boot or runtime attestation.
- Verify the ****Properties**** tab of the asset.

If there is a boot failure, the cause of the error appears. For example:

```
`boot-is-tampered true boot-tamper-details: \"PCR8 mismatched.\"`
```

For a run-time failure, the cause of the error appears. For example:

```
` `` `Bash
runtime-is-tampered true runtime-tamper-details: \"Files with mis-matched
↪ digests: /etc/chrony.conf\"
` `` `
```

Applying a Security Profile on Multiple Gateway Devices Using Campaigns

When you upgrade the firmware or apply security patches to your gateway, the golden profile of your gateway changes, but this action does not qualify as file tampering. To avoid attestation failures for such instances, create a security profile corresponding to the change and apply it to all the gateway devices that require an upgrade using campaigns.

1. Create a security profile corresponding to the file change.
2. Create an IoTC Package with a label added to the package-spec.yml file. For example:

```
` `` `{.sh}
\\# This is a simple array of strings which are just that - labels by
    \\# which you could search a package in SmartHub INFER IoT Center
    labels:
        - security-profile-id: eaa7f966-2915-480f-bf73-2524e019a96d`
```


Note: The `security-profile-id: <label>` must match the security profile ID that you create in step 1.

3. Upload the package to INFER™. For more information about uploading the IoT Package, see [Uploading the IoT Package](#).
4. To apply updates to all gateway devices that require an update, create a campaign with the appropriate query. For information about creating campaigns, see [Creating a Campaign](#).
5. Run the campaign.
6. After the campaign runs successfully, click an updated gateway device and verify that the `security-profile-id` is updated under **Custom Properties**.

Note: For the attestation configuration to take effect, you must reboot the upgraded devices by running the following script when the campaign is in the **ACTIVATE** phase:

```
now="date"
echo $now >> /tmp/activation.log 2>&1
echo "Starting Activation for Updating Security Profile"
>> /tmp/activation.log 2>&1

sudo shutdown -r +1 >> /tmp/activation.log 2>&1

echo 0
```

You have successfully applied a security profile across multiple gateway devices using campaigns.

22 Tasks

The **Tasks** tab provides a view of all the tasks run by administrator. It lists the tasks with the overall progress, user name, organization, and time of creation of the task.

Prerequisite: You must have **View Tasks** permissions to perform this operation.

The Tasks tab displays basic information and entities of the asset commands you send from .

1. To verify the basic information of a task, from the Console, go to **Tasks**.
The list of all the tasks appear.
2. From **Search**, search and click the task name.
Basic information of the task such as:
 - **Task Name**
 - **Task Id**
 - **Progress** (Completed/Skipped/Pending/Failed)
 - **Name** of the command run
 appears at the asset level.
3. To view the progress of the command on each asset, select **Entities**.
The list of assets on which the command is run is displayed. The status of the command such as Completed/Skipped/Pending/Failed appears against each asset.
4. Click the **Asset** name.
The **Inventory - Monitored Assets** page appears.
5. To verify the progress of the command, click .. drop-down menu and select **Commands**.
Command history with the status appears.

22.1 Integrating with ServiceNow

You can integrate SmartHub INFER™ IoT Center with a ServiceNow instance.

SmartHub INFER™ IoT Center provides an integration mechanism with ServiceNow to manage your device alerts. When an alert is generated for a device, it creates an incident in the ServiceNow instance.

This section lists the prerequisites and steps to integrate your SmartHub INFER™ IoT Center instance with ServiceNow.

Pre-Requisites

You must have access to the following instances:

- SmartHub INFER™ IoT Center console
 - ServiceNow
1. Log in to the INFER™ UI and navigate to **Templates > Notifications**.
 2. To create a notification definition, click **CREATE**.
The Create Notification Definition wizard is displayed.
 3. In the **Details** step, enter the name of your notification definition, an optional description, and click **NEXT**.
 4. In the **Settings** step, select **REST Notification**.
 5. Select Notification Categories as **Device Alert** and enable **Secure Protocol**.
 6. Enter the Host URL of the ServiceNow instance. For example, dev79872.service-now.com. Enter the port number as 443.

7. In the URL field, append the URL with the path `/api/now/table/incident`.
8. Copy the security certificate, that is the Root CA from the ServiceNow browser and paste it in the **Certificate** text box.
9. Select the **Authentication Type** as **Basic** and enter your ServiceNow credentials in the **Username** and **Password** text boxes.
10. Under **Advanced Settings**, add a two Headers with the header name as *Content-Type* as *application/json*. Enter the header value as *Host*. For example *host = dev249854.service-now.com*. Click **DONE**.
11. In the **Body Template** text box, enter the keys to be populated in ServiceNow. You can derive the keys from the ServiceNow instance. The following example illustrates a sample body template:

```
{
  "caller_id": "Test User",
  "short_description": "Notification for Alert ${alertState}",
  "description": "This is an automated notification from SmartHub INFER IoT
  ↪ Center.\n\n Device Id : ${deviceId}, \n deviceTemplateId:
  ↪ ${deviceTemplateId}, \n Alert Name : ${alertTemplate}, \n Alert State :
  ↪ ${alertState}, \n Severity : ${alertSeverity}, \n Recommendation :
  ↪ ${recommendation}, \n Alert Definition ID : ${alertDefinitionId}, \n Metric
  ↪ Value : ${lambda}. \n\n To view additional details, go to the SmartHub
  ↪ INFER IoT Center Server."
}
```

12. Click **NEXT**.
13. On the Link page, you have an option to select a notification:
 - Send a notification when there is a success
 - Send a notification when there is a failure and you can use an alternate notification definition.
 - Send a notification when you want to debug any sort of error.
14. Click **NEXT**.
15. On the **Review** tab, review the details and click **SAVE**.

Note : ServiceNow provides multiple tables to which you can insert or create a record. In this example, we use the **Incident** table to create a record. To view the full list of tables in ServiceNow, go to the ServiceNow instance and navigate to REST API Explorer.

You have successfully integrated SmartHub INFER™ IoT Center with ServiceNow. When you associate an alert definition with this ServiceNow notification definition, ServiceNow files an incident whenever an alert is triggered.

23 SmartHub INFER™ In-Product Help

SmartHub INFER™ provides in-product help, allowing you to easily enter queries related to a selected application or service directly from the UI. Follow these steps to report an issue or bug effectively:

23.1 How to Submit a query or Report a Bug in SmartHub INFER™ ?

1. To open the support wizard, click on the messenger icon on the right bottom on the INFER™ UI.
2. To request for support, on the **Support** page, click **Request for Support**.
3. Under the **Choose Topic** drop-down menu, select a topic.
4. Enter a short, clear summary, under the **Summary** textbox.
5. Enter a description, explaining the problem, including when and how the error occurs.
6. If an error or bug appears on the screen, you can either capture a screenshot directly or attach an existing one to illustrate the issue. Click **Capture Screen** of the generated error or click **Browse** to a file that you want to upload.
7. Once all details are entered, click **Submit**.

Request for support ✕

Choose Topic

Dashboard ▾

Summary *

Widget has an error

Description *

Summarize the error here

SCREENSHOT CAPTURED ✕

Attach a file

Choose file... Browse

CANCEL SUBMIT

23.2 Landing Page within INFER™ UI

The **Landing Page** option in INFER™ displays the most up-to-date menu elements. This feature allows you to set a specific page as your fixed home screen upon logging in. The

landing page feature lists the required menu elements that you view on the left navigation panel on the INFER™ UI.

1. To update your main view with Landing Page, click on your profile on the top right corner and select **Landing Page**.

The Change Landing Page window will appear.

2. Select the page you want to set as your home screen.
3. Click **Submit**.

24 Audit Logs

The **Audit Log** module is a critical component for maintaining security, compliance, and operational transparency of INFER™. It records a detailed history of actions performed by all users and devices within INFER™, allowing its administrators to track and review activities for troubleshooting, security analysis, and compliance auditing.

24.0.1 Viewing Logs

Audit Type	Entity Type	Audit Info	Accessor	Organization	Created (IST)
Entity Updated	Device	System property	-	Ajith	12/15/2024, 5:43 PM
Entity Updated	Device	System property	-	Ajith	12/15/2024, 5:43 AM
Entity Updated	Device	System property	-	Ajith	12/15/2024, 5:42 AM
Entity Updated	Device	System property	-	Ajith	12/14/2024, 5:42 PM
Entity Updated	Device	System property	-	Ajith	12/14/2024, 7:49 AM
Entity Updated	Device	System property	-	Ajith	12/14/2024, 7:48 AM
Entity Updated	Device	System property	-	Ajith	12/13/2024, 5:42 PM
Entity Updated	Device	System property	-	Ajith	12/13/2024, 5:42 AM
Entity Updated	Device	System property	-	Ajith	12/13/2024, 5:42 AM
Entity Updated	Device	System property	-	Ajith	12/12/2024, 5:42 PM
Entity Updated	Device	System property	-	Ajith	12/12/2024, 5:42 AM
Entity Updated	Device	System property	-	Ajith	12/12/2024, 5:42 AM
Entity Updated	Device	System property	-	Ajith	12/11/2024, 5:43 AM

You can filter the audit logs based on the following parameters:

- Entity Type
- Audit Type
- Device
- Date Range

Prerequisite: You must have the VIEW_AUDIT_LOGS permission to perform this operation.

To view more details about an entity and audit type, click a search result. For example, when you edit a device or a device template, you can view additional information about the changes made under the **Audit Details** section.

To export audit logs in the **CSV** format, perform the following steps:

1. From the **Audit Log** page, click **EXPORT**.
2. Select **All** to export all audit logs, or **Time Range** to select audit logs within a time range.
3. Click **EXPORT**.

25 Glossary

Some of the terminologies that are frequently used in this guide are described in this section.

Gateway

A Gateway is a physical or virtual device that serves as a connection point between the cloud (public or on premises) and controllers, sensors, and intelligent devices. All data moving to and from the cloud goes through the Gateway. The INFER™ Agent runs and collects information on behalf of other connected Thing devices through the Gateway.

Connected Asset or Thing Asset

A connected device or a Thing device is a nonstandard computing device that can transmit data and is connected to a Gateway. The Thing device connects to a Gateway and sends information to the Server through the SDK Client that is running on the Gateway.

Registered Asset

A registered device is a virtual Gateway that is created on the Server. A registered device does not have a physical Gateway associated with it.

Enrolled Asset

A registered Gateway is enrolled when a physical Gateway is associated with it.

INFER™ Agent

The Agent is a component that resides in the Gateway. It connects the services to run commands and to send operational metrics to the IoTC services. The Agent offers an SDK that exposes APIs. Third-party applications can use these APIs on the Gateway to interact with INFER™.