



SmartHub INFER™



User Guide

Last updated on 21-Mar-24

Find out more about our products & solutions at smarthub.ai/
Copyright © 2024, SmartHub, Inc. All rights reserved.

Contents

1 Introduction	1
1.1 Document Conventions	1
1.2 Privacy Notice	2
1.3 Trademarks	2
1.4 Browser Support	2
1.5 Username Requirements	2
1.6 Password Requirements	3
1.7 Roles and Permissions	3
1.8 Terminology	5
1.9 Typical Use Cases	6
2 Setting up Your Organization	12
2.1 Organizations	12
2.2 Users	15
2.3 Groups	17
2.4 Roles	19
3 Managing Dashboards & Widgets	22
3.1 Working with Widgets	22
3.2 Create a Dashboard	22
3.3 Create a Widget	23
4 Working with Insights	25
4.1 Viewing Dashboards	25
4.2 Customizing Dashboards	28
4.3 Downloading Data from Table Panels	30
5 Spaces	32
5.1 Creating Spaces	32



5.2 Editing Spaces.....	33
5.3 Assigning / Unassigning Parent Spaces.....	34
5.4 Bulk Assign Spaces to Devices.....	36
5.5 Deleting Spaces.....	38
6 Space Management.....	40
6.1 Smart Spaces.....	40
6.2 Use Cases.....	40
6.3 What is a Space Template?.....	43
6.4 Creating a Space Template.....	43
6.5 Editing a Space Template.....	45
6.6 Assigning a Parent Template.....	45
6.7 Cloning a Space Template.....	46
6.8 Deleting a Space Template.....	48
7 Working with Device Templates.....	50
7.1 What is a Device?.....	50
7.2 What is a Device Template?.....	51
7.3 What are Device Properties?.....	51
7.4 What are Metrics?.....	52
7.5 INFER™ Agent Daemon.....	52
7.6 Editing a Device Template.....	60
8 Onboarding Gateways.....	63
8.1 What is a Gateway?.....	63
8.2 Onboarding a Gateway using Basic Authentication.....	66
8.3 Onboarding a Gateway using Token-Based Authentication.....	68
8.4 Onboarding a Gateway using Property-based Authentication.....	70
8.5 Onboarding a Gateway using TPM-based Authentication.....	72
8.6 Onboarding a Gateway using Zero Touch Enrollment.....	75
8.7 Whitelisting a Device.....	76

8.8 Registering Multiple Devices using CLI.....	76
8.9 Registering Multiple Gateways.....	81
9 Working with INFER™ Agent.....	84
9.1 Installing INFER™ Agent.....	84
9.2 Working with IoTCAgent CLI.....	89
9.3 Updating INFER™ Agent.....	90
10 Onboarding Connected Things.....	94
10.1 Registering Things One by One.....	94
10.2 Registering Things in Bulk.....	98
11 Working with Devices.....	101
11.1 Device States.....	101
11.2 Sending a Command to INFER™ Agent.....	102
11.3 Sending a Command to Multiple Devices.....	103
11.4 Bulk Command Cancellation.....	104
11.5 Viewing List of Files.....	105
11.6 Viewing List of Devices by State.....	105
11.7 Viewing List of Devices by Property.....	106
11.8 Updating Bulk Custom Properties on Multiple Devices.....	106
11.9 Editing Custom Properties via CSV.....	108
11.10 Collecting Metrics using DefaultClient Binary.....	110
11.11 Viewing Metric Graphs.....	111
11.12 Assigning Spaces to Devices.....	112
11.13 Unassigning Spaces to Devices.....	115
11.14 Unenrolling a Device.....	117
11.15 Deleting Single or Multiple Devices.....	117
12 Device Maintenance.....	119
12.1 Entering Maintenance.....	119
12.2 Exiting Maintenance.....	120



13 Device Migration.....	123
13.1 Migration Checklist.....	124
13.2 Migrating Things & Gateways.....	125
14 Working with Asset Ledger.....	127
14.1 Creating an Asset Folder.....	128
14.2 Modifying the Default Field Group.....	130
14.3 Creating a New Field Group.....	131
14.4 Moving Fields between Groups.....	132
14.5 Working with Asset Tables.....	132
14.6 Adding Assets.....	138
14.7 Importing Assets.....	139
14.8 Editing Asset Folders.....	139
14.9 Deleting Asset Folders.....	140
15 Working with Campaigns.....	141
15.1 What is a Campaign?.....	141
15.2 Campaign Approvals.....	142
15.3 Campaign State Transition Scheme.....	144
15.4 Creating a Campaign.....	144
15.5 Starting the Campaign.....	147
15.6 Cloning a Campaign.....	148
15.7 Editing a Campaign.....	151
15.8 Deleting a Campaign.....	151
16 Using Advanced Search.....	153
16.1 Saving a Filter Definition.....	153
17 Working with Package Builder.....	155
17.1 What is a Package?.....	155
17.2 Building a Package.....	155

18 Package Management CLI for Advanced Users.....	160
18.1 Creating a Specification YML File.....	160
18.2 Downloading the Package Management CLI Tool.....	167
18.3 Generating an IoTCP Package.....	167
18.4 Sample Script for Running a Campaign on a Thing Device... <td>173</td>	173
19 Controlling a Campaign using DefaultClient CLI.....	177
19.1 Running a Campaign using Default Properties.....	177
19.2 Running a Campaign in On-Demand Mode.....	178
19.3 Running a Campaign in Headless Mode.....	181
19.4 Approving the OTA Update Phases.....	181
20 Working with Alerts & Notifications.....	183
20.1 What is an Alert?.....	183
20.2 What is an Alert Definition?.....	185
20.3 Creating an Alert Definition.....	186
20.4 Editing an Alert Definition.....	190
20.5 Disabling an Alert Definition.....	191
20.6 Enabling an Alert Definition.....	192
20.7 What is a Notification?.....	193
20.8 What is a Notification Definition?.....	194
20.9 Creating a Notification Definition.....	195
20.10 Editing a Notification Definition.....	198
20.11 Cloning a Notification Definition.....	199
20.12 Deleting a Notification Definition.....	200
21 Working with API Keys.....	202
21.1 Creating a Key.....	202
21.2 Editing a Key.....	204
21.3 Renewing a Key.....	205
21.4 Revoking a Key.....	206



21.5 Deleting a Key.....	207
21.6 Viewing Key Details.....	208
21.7 Viewing Key Permissions.....	209
21.8 Viewing Key History.....	210
21.9 Key States.....	210
22 Settings.....	211
22.1 Setting up Custom Branding.....	211
22.2 Setting up the Default Gateway & Thing Template.....	213
22.3 Setting up Audit Log Retention Period.....	214
22.4 Setting up Identity & Access.....	215
22.5 Setting up Insights Dashboard.....	219
22.6 Setting up Notification Retention Period.....	220
22.7 Setting up Notification Definitions.....	220
22.8 System Notifications Settings.....	221
22.9 Setting up OTA Updates.....	222
23 Audit Logs.....	224
24 Tasks.....	225
25 TPM-Based Attestation.....	226
25.1 What is Boot Attestation?.....	226
25.2 What is Runtime Attestation?.....	227
25.3 What Is IMA.....	228
25.4 Preparing Your Gateway for Boot Attestation.....	228
25.5 Preparing Your Gateway for Runtime Attestation.....	228
25.6 Create a Boot Attestation Profile.....	231
25.7 Create a Runtime Attestation Profile.....	232
25.8 Associate the Attestation Profile With the TPM-Based Template.....	233
25.9 Applying a Security Profile on Multiple Gateway Devices Using Campaigns.....	235

26 Integrating with ServiceNow.....	238
27 Integrating with Third-Party CMS.....	241
28 Troubleshooting.....	242
28.1 Troubleshooting Campaign Management.....	242
28.2 INFER™ Agent Connectivity to the INFER™ Server.....	243

1 Introduction

INFER™ is an IoT & Edge management solution that improves an enterprise's operational excellence and cost efficiency.

INFER™ on-boards, configures, manages, monitors, and secures unmanned IoT devices and objects at scale. The solution 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:

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

Over The Air (OTA) Campaign - Software, Firmware, Operating System, and BIOS Updates - Package Repository and Updates

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

1.1 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.

1.2 Privacy Notice

INFER™ has the ability to collect data from IoT and end-user devices as configured by you. When using INFER™, 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 please read [SmartHub's Privacy Policy](#).

1.3 Trademarks

Copyright © 2023, SmartHub, Inc. All rights reserved.

1.4 Browser Support

The INFER™ supports the latest versions of the following browsers: Mozilla Firefox, Google Chrome, Microsoft Edge web browsers.



Internet Explorer and Safari browsers are not supported.

1.5 Username Requirements

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

Username can not contain more than one special character.

This check is for both local user and SSO user.

1.5.1 Local User

As a local user, you can:

-
- choose a username 1–50 characters long.
 - use alphanumeric values along with one of the following special characters listed below:
 - underscore (_),
 - hyphen (-), and
 - period (.)

1.5.2 SSO User

As a SSO user, your username must contain only one of the following special characters listed below:

- underscore (_),
- hyphen (-), and
- period (.)

All other special characters are disallowed.

1.6 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: @#\$*!^

1.7 Roles and Permissions

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

1.7.1 Roles

INFER™ provides the following default roles:

Role Descriptions

Default Role	Description
Identity & Access Administrator	Add or modify an organization, add or modify users, groups, roles, and notifications, and view audit logs
Campaign Administrator	Add or modify campaigns, packages for OTA updates, and view notification definitions and notification destinations
Package Administrator	Add or delete packages
Device Administrator	Add or modify devices and device templates
Gateway Administrator	Add devices, create device tokens and credentials, and view device templates
Alert Administrator	Can acknowledge alerts and view alerts, organizations users, roles, groups, devices, device templates, notifications, and so on. This is a view only role.
Monitoring Administrator	Can modify alerts and notifications, and view metrics
Asset ledger Admin	Create, view and edit Asset related data
Edit Sensitive Properties	Create, view and edit a Device's properties that are flagged as sensitive
Insights Viewer	Can view various Dashboards under the Insights menu
Insights Editor	Can create, view and edit Dashboards under the Insights menu
View-Only User	Has 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**.

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

Group	Roles
Organization Administrators	<ul style="list-style-type: none"> • Identity & Access Administrator

System Administrators	<ul style="list-style-type: none"> • Campaign Administrator • View Organization • Package Administrator • Device Administrator • Gateway Administrator • Alert Administrator • Monitoring Administrator • Asset Ledger Administrator • Edit Sensitive Properties • Insights Viewer
Data Extraction Group	<ul style="list-style-type: none"> • View-Only User



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

1.8 Terminology

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 Device or Thing Device

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 INFER™ SDK Client that is running on the Gateway.

Registered Device

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 Device

A registered Gateway is enrolled when a physical Gateway is associated with it.

INFER™ Agent

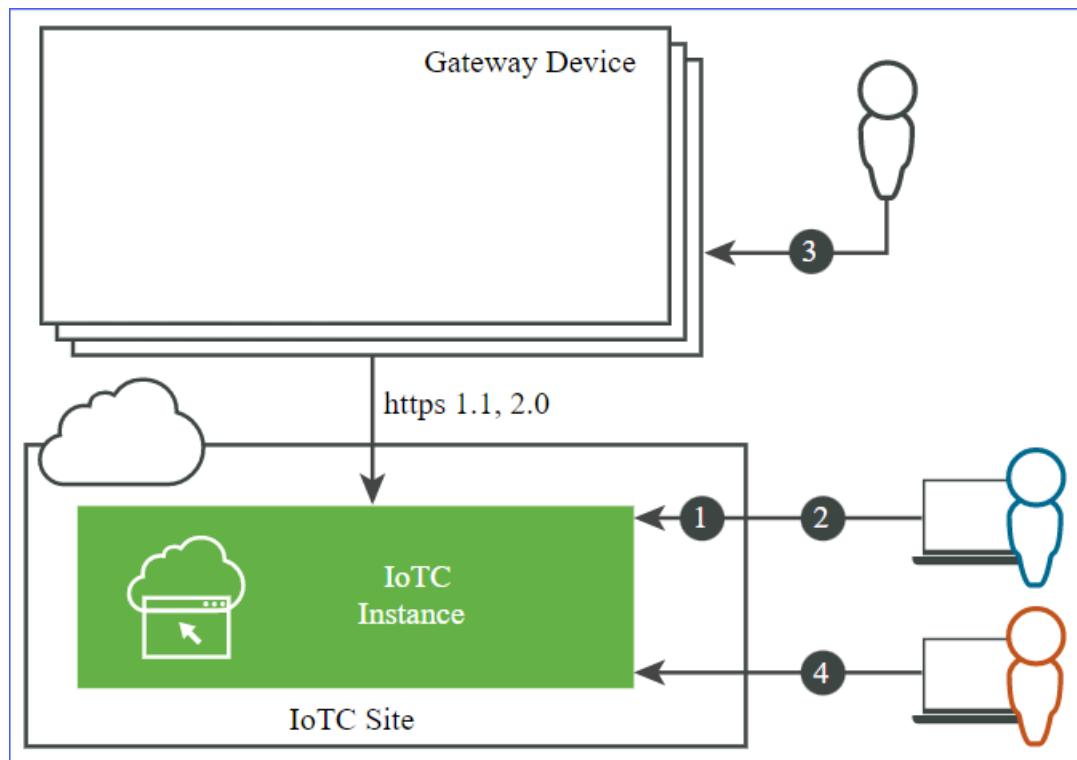
The INFER™ Agent is a component that resides in the Gateway. It connects the INFER™ services to run commands and to send operational metrics to the IoT services. The INFER™ Agent offers an SDK that exposes APIs. Third-party applications can use these APIs on the Gateway to interact with INFER™.

1.9 Typical Use Cases

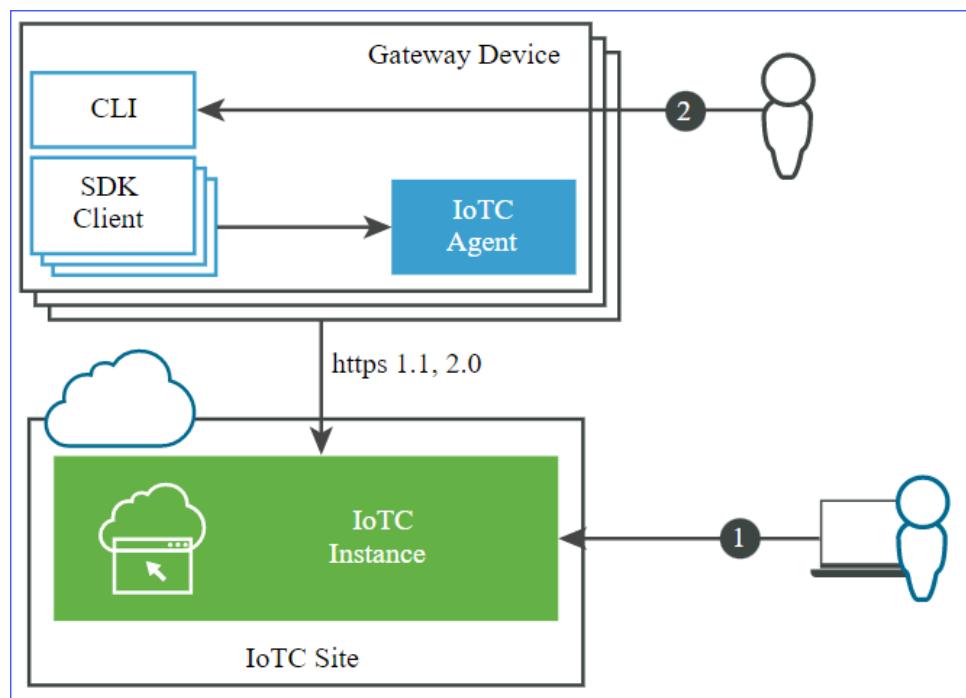
You can perform the following role-specific operations with INFER™.

1.9.1 Setting Up INFER™

1. Organization Administrator creates organizations.
2. Organization Administrator creates users and assigns roles.
3. Gateway Administrator installs and powers on the Gateway.
4. Device Administrator creates device templates.



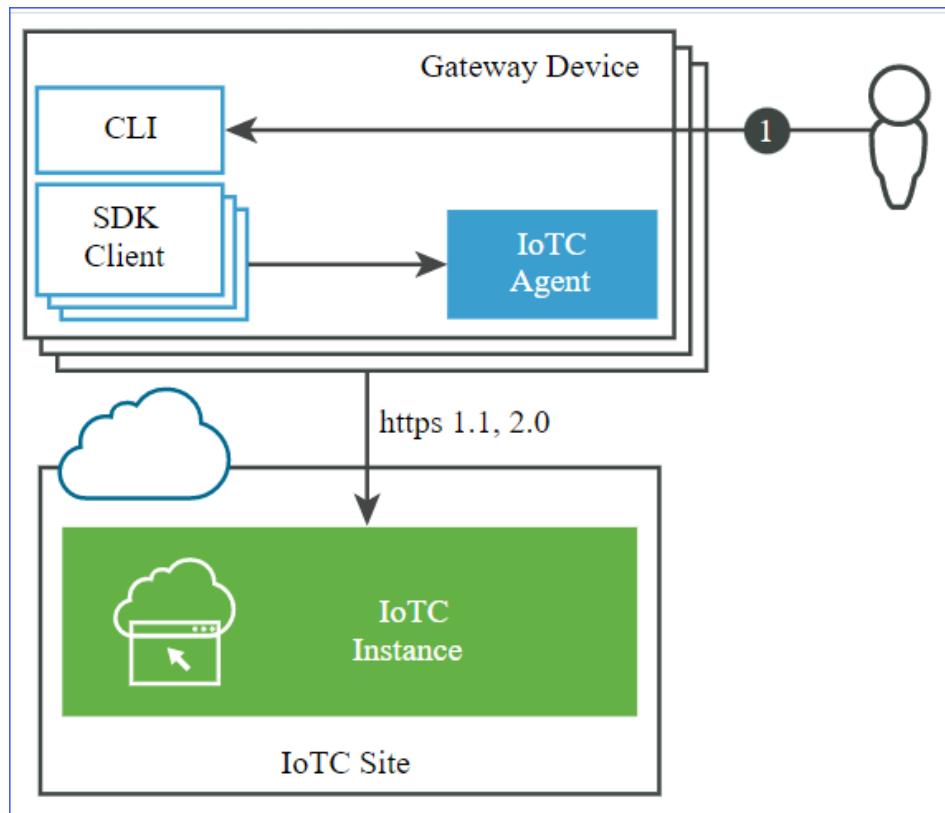
1.9.2 Enrolling a Registered Device





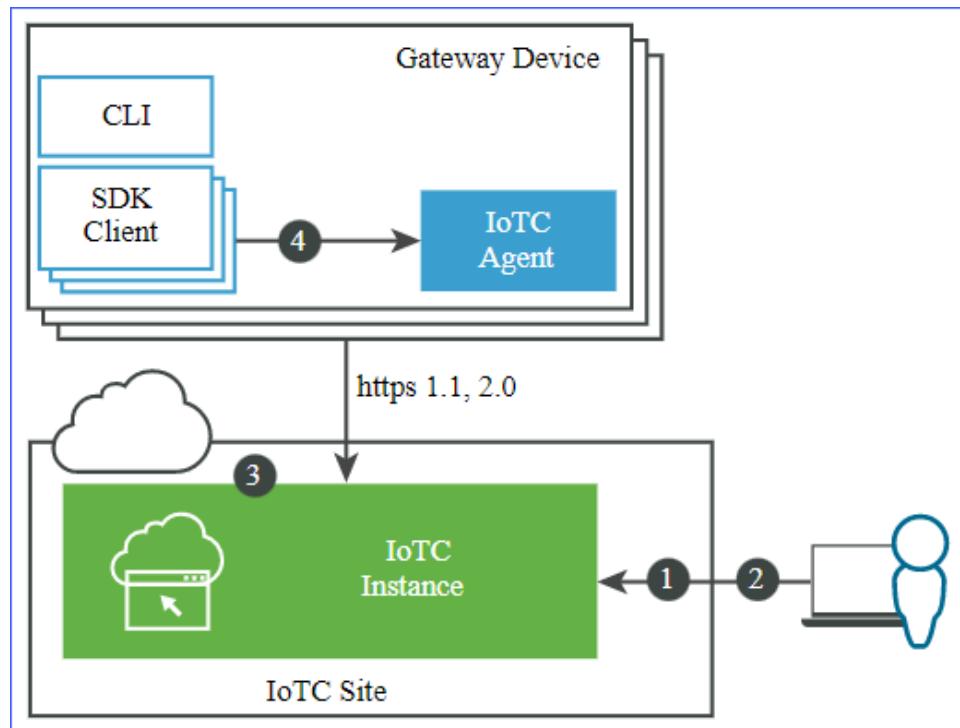
1. Device Administrator registers a device through the INFER™ Console or through the API.
2. Gateway Administrator installs the INFER™ Agent on the Gateway.

1.9.3 Enrolling a Non-Registered Device



1. Gateway Administrator enrolls the Gateway using the template name, user name, and credentials.

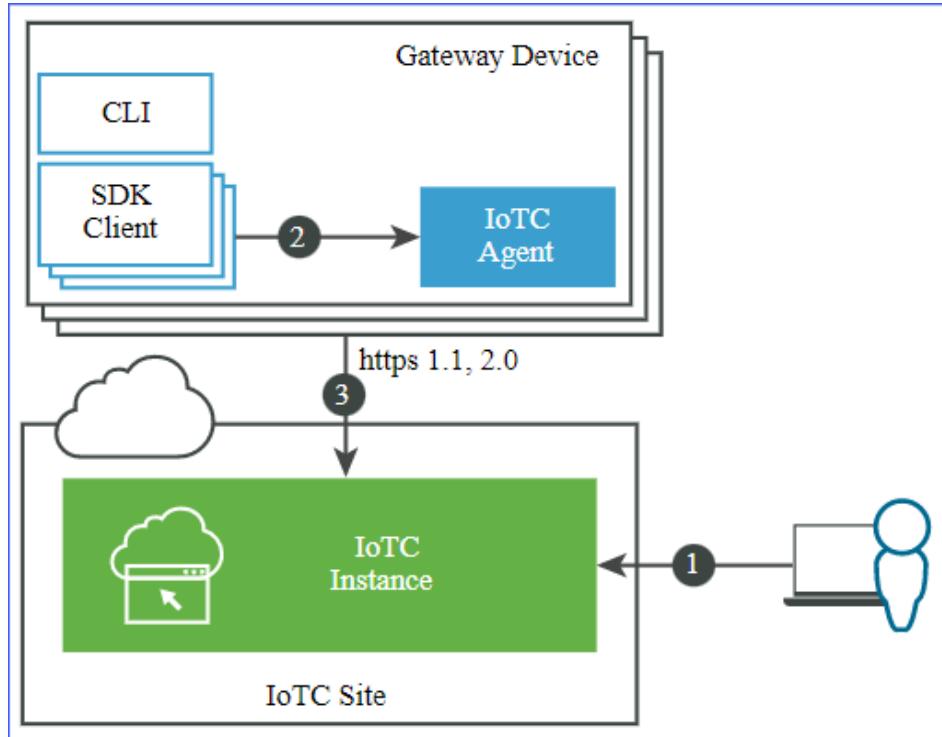
1.9.4 Controlling a Device



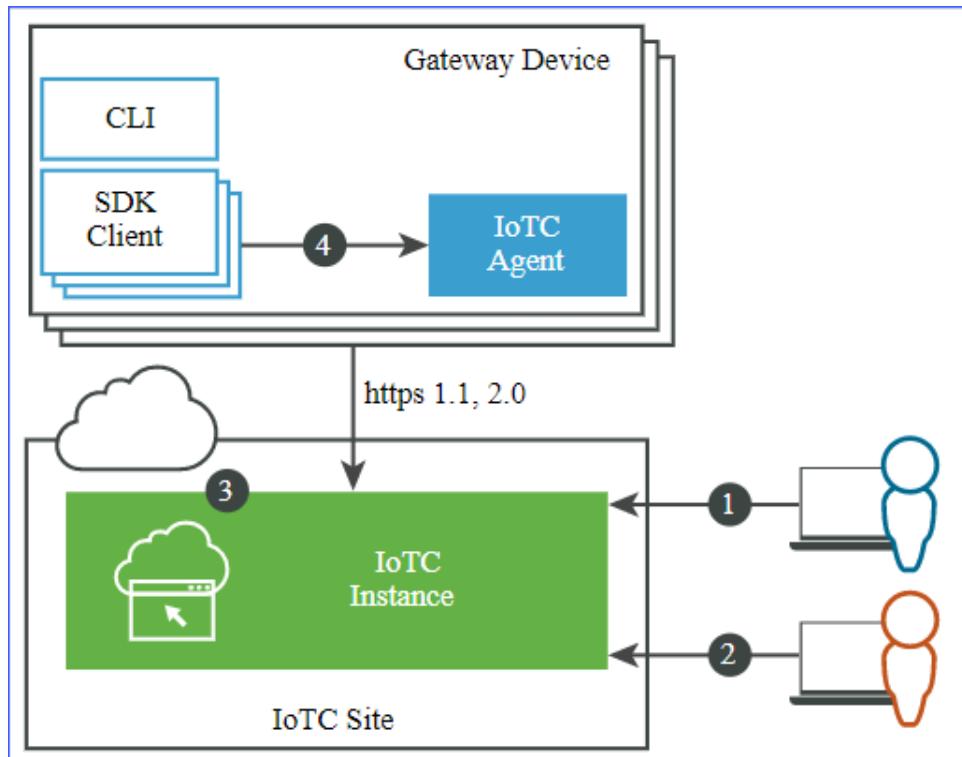
1. Device Administrator configures the device template with the allowed commands.
2. Device Administrator selects a device and sends a command.
3. The Server pushes the command to the INFER™ Agent. If the agent is not connected to the Server, the Server queues the command.
4. The INFER™ Agent receives and runs the command, or delegates the command to the SDK Client.

1.9.5 Working with Metrics

1. Device Administrator configures the metrics to be collected in the device template.
2. The SDK Client collects and publishes the metrics.
3. The INFER™ Agent transfers the metrics to the IoTC instance

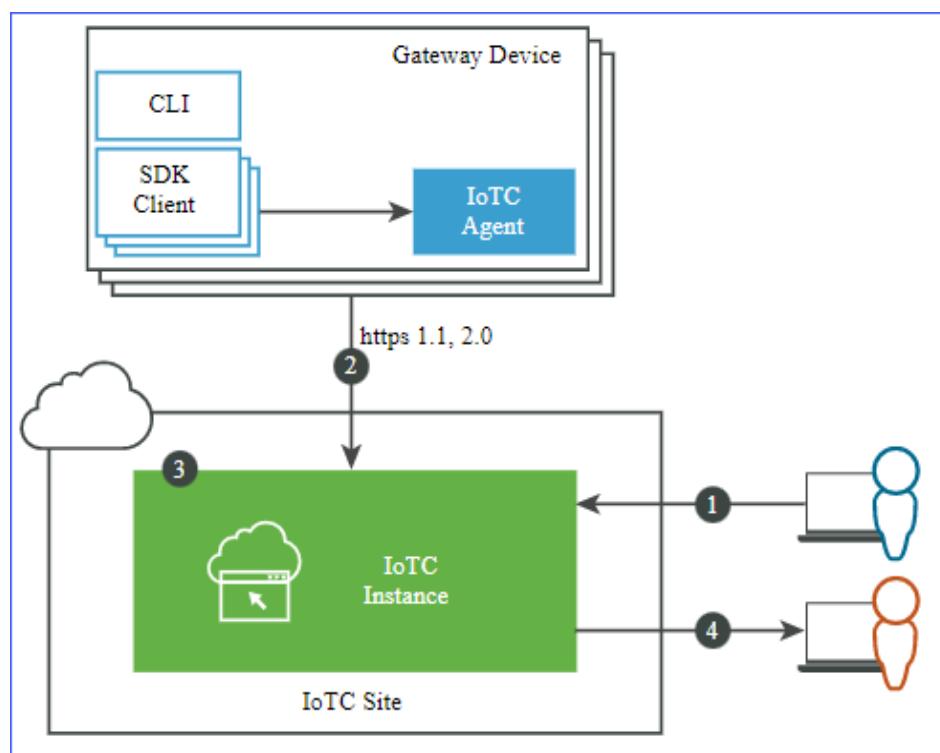


1.9.6 Configuring Over The Air Updates



1. Package Administrator creates and uploads update packages.
2. Campaign Administrator creates and starts a campaign to update selected devices with the packages.
3. The Server evaluates the active campaigns and queues the update for the device.
4. The INFER™ Agent downloads, installs, and activates the package. Or, it delegates the command to the SDK Client.

1.9.7 Working with Alerts and Notifications



1. Monitoring Administrator configures the alert definitions and notification definitions.
2. The INFER™ Agent publishes metrics from the enrolled Gateway.
3. The Server evaluates the alert definitions, raises, and sends alert notifications.
4. Alert Administrator acknowledges the alert and initiates action.

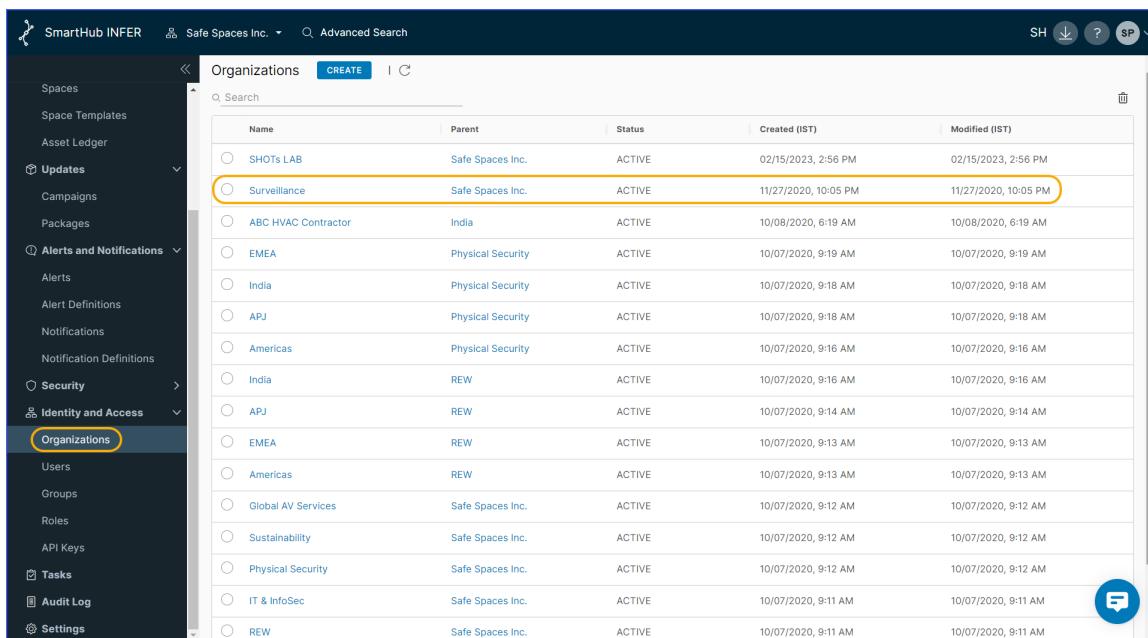
2 Setting up Your Organization

This chapter details the concepts and steps to configure Organizations, Users, Groups, and Roles from INFER™.

Users authenticate at the organization level, supplying credentials established by an organization administrator when the user was created or imported. System administrators create and provision organizations, while organization administrators manage organization users, groups, and devices.

2.1 Organizations

Use the **Organizations** tab to manage your organization's users and devices.



Name	Parent	Status	Created (IST)	Modified (IST)
SHOTS LAB	Safe Spaces Inc.	ACTIVE	02/15/2023, 2:56 PM	02/15/2023, 2:56 PM
Surveillance	Safe Spaces Inc.	ACTIVE	11/27/2020, 10:05 PM	11/27/2020, 10:05 PM
ABC HVAC Contractor	India	ACTIVE	10/08/2020, 6:19 AM	10/08/2020, 6:19 AM
EMEA	Physical Security	ACTIVE	10/07/2020, 9:19 AM	10/07/2020, 9:19 AM
India	Physical Security	ACTIVE	10/07/2020, 9:18 AM	10/07/2020, 9:18 AM
APJ	Physical Security	ACTIVE	10/07/2020, 9:18 AM	10/07/2020, 9:18 AM
Americas	Physical Security	ACTIVE	10/07/2020, 9:16 AM	10/07/2020, 9:16 AM
India	REW	ACTIVE	10/07/2020, 9:16 AM	10/07/2020, 9:16 AM
APJ	REW	ACTIVE	10/07/2020, 9:14 AM	10/07/2020, 9:14 AM
EMEA	REW	ACTIVE	10/07/2020, 9:13 AM	10/07/2020, 9:13 AM
Americas	REW	ACTIVE	10/07/2020, 9:13 AM	10/07/2020, 9:13 AM
Global AV Services	Safe Spaces Inc.	ACTIVE	10/07/2020, 9:12 AM	10/07/2020, 9:12 AM
Sustainability	Safe Spaces Inc.	ACTIVE	10/07/2020, 9:12 AM	10/07/2020, 9:12 AM
Physical Security	Safe Spaces Inc.	ACTIVE	10/07/2020, 9:12 AM	10/07/2020, 9:12 AM
IT & InfoSec	Safe Spaces Inc.	ACTIVE	10/07/2020, 9:11 AM	10/07/2020, 9:11 AM
REW	Safe Spaces Inc.	ACTIVE	10/07/2020, 9:11 AM	10/07/2020, 9:11 AM

2.1.1 Viewing Organization Details

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

You must have the `VIEW_ORGANIZATION` permission to perform this operation.

- From the INFER™ Console, go to **Organizations** as highlighted above.

The Organizations page displays your organizations, sub organizations, and their



status.

2. To view more details about an organization, click the organization name.

Details about the organization are displayed.

Section	Information displayed
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.
Devices	Displays the device information such as device 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.

2.1.2 Creating an Organization

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

You must have the permissions associated with the Organization Administrator role to perform this operation. For more information about roles and permissions, see "Roles and Permissions" on page 3.

1. From the INFER™ Console, go to **Identity & Access > Organizations**.

The Organizations page is displayed.

2. Click **CREATE**.

The **Create Organization** wizard is appears.

3. In the **Basic Information** step, perform the following steps:

1. Enter the name of your organization.

2. Select the parent organization from the **Parent Organization** drop-down.



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

3. 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.



Organization Identifier is not a mandatory field.

4. Click **Next**.

4. In the **Review** step, review the information that you have entered and click **SAVE**.

You have successfully created an organization.

2.1.3 Editing an Organization

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

You must have the permissions associated with the Organization Administrator role to perform this operation. For more information about roles and permissions, see "Roles and Permissions" on page 3.

1. From the INFER™ Console, go to **Identity & Access > Organizations**.

The Organizations page appears.

2. Click the organization to edit.

The details of the organization are displayed.

3. From the **Actions** drop-down, click **Edit**.

The Edit Organization window appears.

4. Update your organization details and click **SAVE**.

You have successfully updated your organization details.

2.1.4 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 are displayed for the current organization and its sub-organizations.

You must be an Identity & Access administrator to perform this operation.

1. From the INFER™ Console, go to **Identity & Access > Organizations** and select your organization.

2. From 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**.

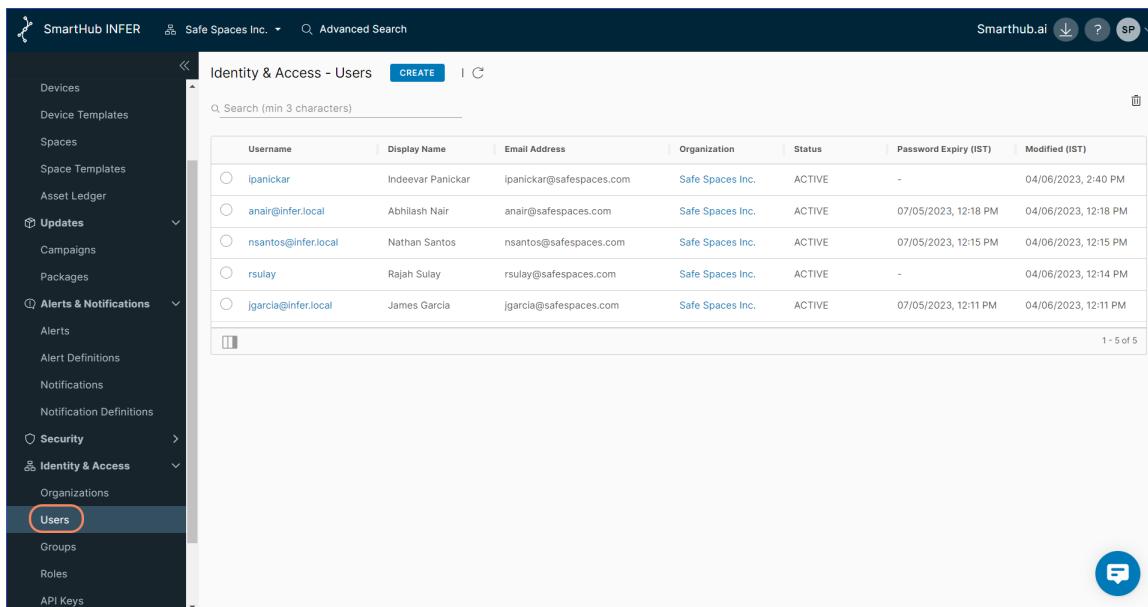
The services and their usage values are displayed.

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™.



Username	Display Name	Email Address	Organization	Status	Password Expiry (IST)	Modified (IST)
ipanickar	Indeever Panicker	ipanickar@safespaces.com	Safe Spaces Inc.	ACTIVE	-	04/06/2023, 2:40 PM
anair@infer.local	Abhilash Nair	anair@safespaces.com	Safe Spaces Inc.	ACTIVE	07/05/2023, 12:18 PM	04/06/2023, 12:18 PM
nsantos@infer.local	Nathan Santos	nsantos@safespaces.com	Safe Spaces Inc.	ACTIVE	07/05/2023, 12:15 PM	04/06/2023, 12:15 PM
rsulay	Rajah Sulay	rsulay@safespaces.com	Safe Spaces Inc.	ACTIVE	-	04/06/2023, 12:14 PM
jgarcia@infer.local	James Garcia	jgarcia@safespaces.com	Safe Spaces Inc.	ACTIVE	07/05/2023, 12:11 PM	04/06/2023, 12:11 PM

1 - 5 of 5

2.2.1 Creating a User

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

You must have the CREATE_USER permission to perform this operation.

1. From the INFER™ Console, go to **Identity & Access > Users**.

The **Identity & Access - Users** page appears.

2. Click **CREATE**.

The **Create User** wizard is displayed.

3. In the **Details** step, enter the following details:

- **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" on page 3.
 - **Confirm New Password** - Confirm the password that you have entered.
- Click **Next**.

4. In the **Groups** step, select the appropriate groups for the user and click **Next**.

5. In the **Review** step, review the information and click **SAVE**.

You have successfully created a user.

2.2.2 Editing a User

This section lists the steps to edit user details from the INFER™ Console.

You must have the `EDIT_USER` permission to perform this operation.

1. From the INFER™ Console, go to **Identity & Access > Users**.

The **Identity & Access - Users** page appears.

2. Click the user to edit.

3. From the **Actions** drop-down, 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

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

You must have the `DELETE_USER` permission to perform this operation.

1. From the INFER™ Console, go 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.
An action confirmation message is displayed.
4. To confirm the action, click **DELETE**. You have successfully deleted a user.



This action deletes the user permanently.

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.

The screenshot shows the SmartHub INFER Identity & Access - Groups page. The left sidebar has a tree view with 'Updates', 'Campaigns', 'Packages', 'Alerts & Notifications', 'Security' (selected), 'Identity & Access' (selected), 'Groups' (highlighted with a red circle), 'Roles', and 'API Keys'. The main content area has a search bar and a table with columns: Name, Description, Organization, Created (IST), and Modified (IST). The table lists various groups like 'Organization Administrators', 'System Administrators', etc. A bottom navigation bar shows '1 - 11 of 11' and a blue message icon.

Name	Description	Organization	Created (IST)	Modified (IST)
Organization Administrators	Organization Administrators	SmartHub	09/20/2020, 12:45 AM	08/23/2023, 12:37 PM
System Administrators	System Administrators	SmartHub	09/20/2020, 12:45 AM	08/08/2023, 4:20 PM
Campaign Team	This team is tasked for carrying out campaigns.	SmartHub	04/06/2023, 3:07 PM	04/06/2023, 3:54 PM
Device Team	This is the Device Team.	Safe Spaces Inc.	04/06/2023, 3:47 PM	04/06/2023, 3:47 PM
Package Team	Team tasked with developing packages.	SmartHub	04/06/2023, 2:56 PM	04/06/2023, 2:56 PM
Technical Customer Service Team	Team responsible for Technical related Customer Services	SmartHub	01/25/2021, 4:15 AM	01/25/2021, 4:15 AM
Read-Only Users		SmartHub	11/19/2020, 9:59 AM	11/19/2020, 9:59 AM
Data Extraction Group	Users with permission to extract data from Infer into other systems	SmartHub	09/25/2020, 12:09 PM	09/25/2020, 12:09 PM
Onboarding Team	Team that onboards devices	SmartHub	09/24/2020, 11:20 PM	09/24/2020, 11:20 PM
Organization Administrators	Organization Administrators	Safe Spaces Inc.	09/24/2020, 10:32 PM	09/24/2020, 10:32 PM
System Administrators	System Administrators	Safe Spaces Inc.	09/24/2020, 10:32 PM	09/24/2020, 10:32 PM

2.3.1 Creating a Group

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

You must have the CREATE_GROUP permission to perform this operation.

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

You have successfully created a user group.

2.3.2 Editing a Group

This section lists the steps to edit user details from the INFER™ Console.

You must have the EDIT_GROUP permission to perform this operation.

1. From the INFER™ Console, go to **Identity & Access > Groups**.
The **Identity & Access - Groups** page appears.
2. Click the group to edit.
3. From the **Actions** drop-down, 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.

You must have the DELETE_GROUP permission to perform this operation.

1. From the INFER™ Console, go 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 is displayed.
4. To confirm the action, click **DELETE**.



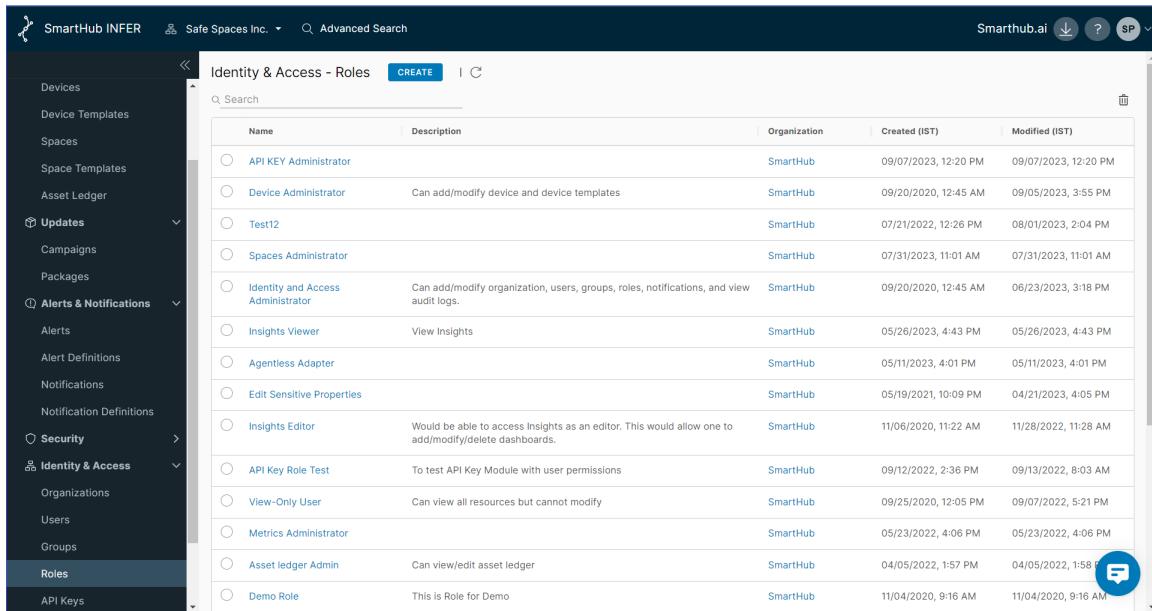
This action deletes the group permanently.

You have successfully deleted the group.

2.4 Roles

When you assign a user or group permissions, you pair the user or group with a role. A role is a predefined set of privileges.

A single user might have different roles. For a list of default roles and their permissions, see "Roles and Permissions" on page 3.



Name	Description	Organization	Created (IST)	Modified (IST)
API KEY Administrator		SmartHub	09/07/2023, 12:20 PM	09/07/2023, 12:20 PM
Device Administrator	Can add/modify device and device templates	SmartHub	09/20/2020, 12:45 AM	09/05/2023, 3:55 PM
Test12		SmartHub	07/21/2022, 12:26 PM	08/01/2023, 2:04 PM
Spaces Administrator		SmartHub	07/31/2023, 11:01 AM	07/31/2023, 11:01 AM
Identity and Access Administrator	Can add/modify organization, users, groups, roles, notifications, and view audit logs.	SmartHub	09/20/2020, 12:45 AM	06/23/2023, 3:18 PM
Insights Viewer	View Insights	SmartHub	05/26/2023, 4:43 PM	05/26/2023, 4:43 PM
Agentless Adapter		SmartHub	05/11/2023, 4:01 PM	05/11/2023, 4:01 PM
Edit Sensitive Properties		SmartHub	05/19/2021, 10:09 PM	04/21/2023, 4:05 PM
Insights Editor	Would be able to access Insights as an editor. This would allow one to add/modify/delete dashboards.	SmartHub	11/06/2020, 11:22 AM	11/28/2022, 11:28 AM
API Key Role Test	To test API Key Module with user permissions	SmartHub	09/12/2022, 2:36 PM	09/13/2022, 8:03 AM
View-Only User	Can view all resources but cannot modify	SmartHub	09/25/2020, 12:05 PM	09/07/2022, 5:21 PM
Metrics Administrator		SmartHub	05/23/2022, 4:06 PM	05/23/2022, 4:06 PM
Asset ledger Admin	Can view/edit asset ledger	SmartHub	04/05/2022, 1:57 PM	04/05/2022, 1:58 PM
Demo Role	This is Role for Demo	SmartHub	11/04/2020, 9:16 AM	11/04/2020, 9:16 AM

2.4.1 Creating a Role

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

You must have the CREATE_ROLE permission to perform this operation.

- From the INFER™ Console, go to **Identity & Access > Roles**.
The **Identity & Access - Roles** page appears.
- Click **CREATE**.
The **Create Role** wizard appears.
- Under **Details**, enter the role name and a short description about the role. Click **Next**.
- Under **Permissions**, select the permissions to assign to the role. Click **Next**.
- Under **Review**, review the information and click **SAVE**.

You have successfully created a role.

2.4.2 Editing a Role

This section lists the steps to edit role details from the INFER™ Console.

You must have the EDIT_ROLE permission to perform this operation.



-
1. From the INFER™ Console, go to **Identity & Access > Roles**.

The **Identity & Access - Roles** page appears.

2. Click the role to edit.
3. From the **Actions** drop-down, 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

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

You must have the **DELETE_ROLE** permission to perform this operation.

1. From the INFER™ Console, go 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 is displayed.
3. To confirm the action, click **DELETE**.



This action deletes the group permanently.

You have successfully deleted a role.

3 Managing Dashboards & Widgets

By default, INFER™ provides a dashboard that displays the important information about your devices, alerts, and campaigns. However, you can also create your own customized dashboards by adding only your desired widgets.

3.1 Working with Widgets

Widgets are small applications on the home screen of the INFER™ that give you quick access to important information about your devices, alerts, and campaigns.

3.2 Create a Dashboard

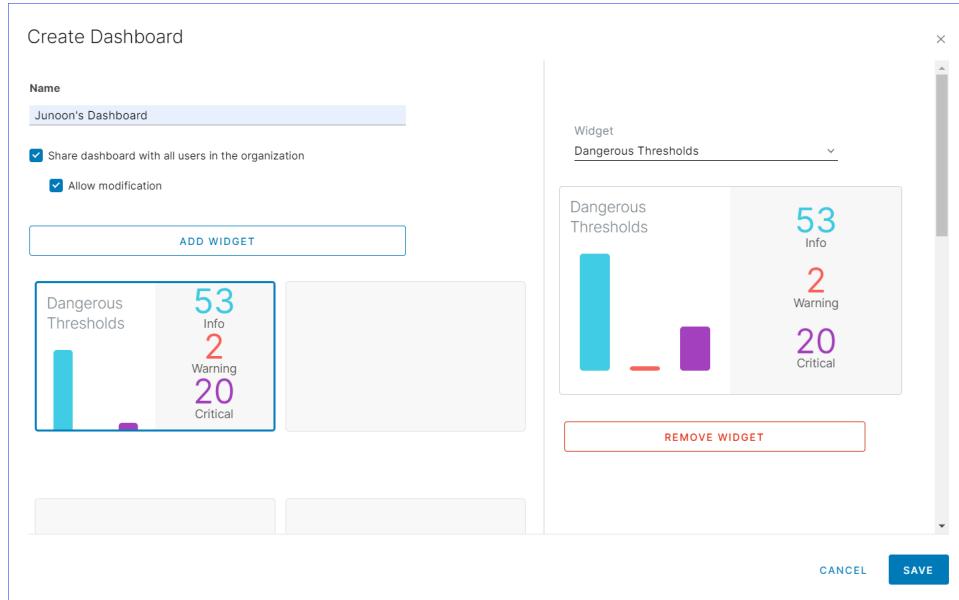
The first step in customizing your dashboard view is to create a dashboard.

You must have the **Create Dashboard** permission to perform this operation.

1. From the INFER™ dashboard page, click the **MANAGE** button.
2. Select **CREATE > Create Dashboard**.

The Create Dashboard wizard is displayed.

3. Enter a name for your dashboard and select the **Share with the organization** check box if you want to share your dashboard with others who have the **View Dashboard** permission within your organization. If you select **Share with the organization**, you can also allow others to modify your dashboard. Select **Allow others to modify**.



4. To start adding the widgets that you created to your dashboard, click **ADD WIDGET**. You can select your **widget** from the **Widget** drop-down on the right.
5. To remove a widget from your dashboard, select the widget and click **REMOVE WIDGET**.
6. Click **SAVE**.

Your dashboard is saved.

You have successfully created a dashboard and added widgets to it.

3.3 Create a Widget

You can create customized widgets to be displayed on your dashboard.

You must have the **Create Dashboard Widget** permission to perform this operation.

1. From the INFER™ dashboard page, click the **MANAGE** button.
 2. Select **CREATE > Create Widget**.
- The Create Widget wizard is displayed.
3. In the **Details** step, enter the following information:

-
- **Name** - Type the name of your widget.
 - To share your widget with others in your organization, select **Share with the organization**. To allow others to modify your dashboard, select **Allow others to modify**.
 - **Select Entity** - Select the entity for which you want to create a widget. The entities are:
 - **Devices** - Creates a device widget.
 - **Alerts** - Creates an alerts widget.
 - **Device Template** - Creates a device template widget.
 - **Campaigns** - Creates a campaigns widget.In this example, we create a **Devices** widget.

4. Select **Devices** and click **NEXT**.
5. In the **Query Group and Chart** step, you can build a query to narrow down the sample set of devices. In **Filter** step:
 1. Select devices of a particular **Device Type**, **Enrollment State**, **Device Template**, and **Properties** to be displayed.
You can search the properties by name and value.
 2. To group the devices according to their **Device Type** or **Enrollment State**, select **Group data**.
 3. Under **Data Visualization**, select a visualization type for your widget.

The count of all devices that meet the query parameters is in your widget.

6. Click **NEXT**.
7. In the **Review** step, review the information that you have entered, and click **SAVE**.

You have successfully created a widget. You can now add the widget to your dashboard.

4 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 variety of panels making it easy 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.

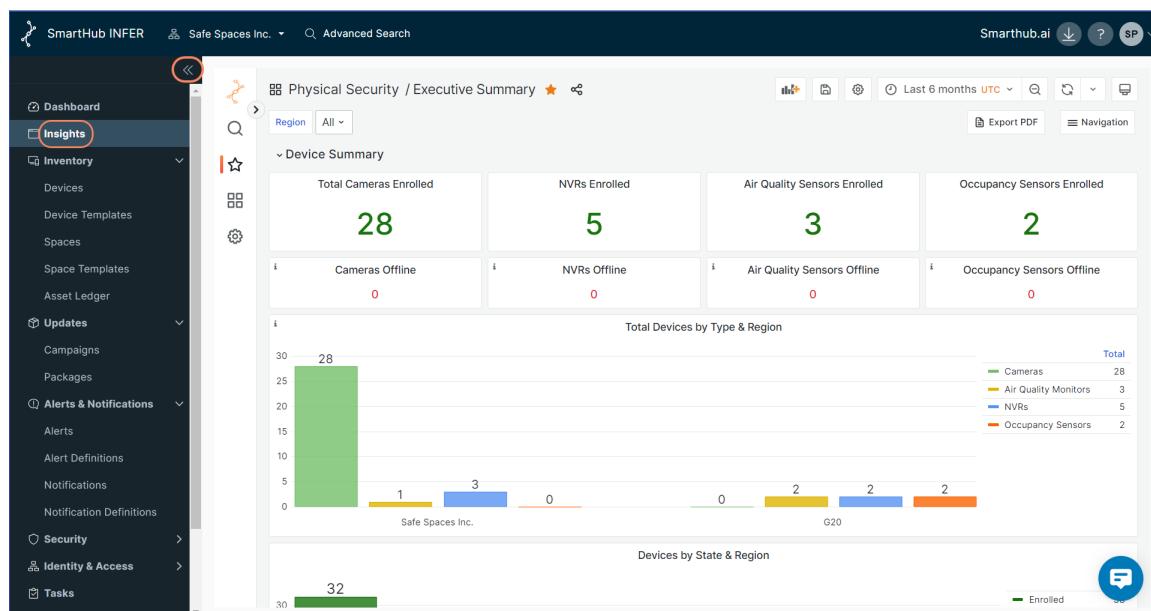
4.1 Viewing Dashboards

To view INFER™'s Insights dashboards, you must have the INSIGHTS_VIEWER permission associated with the Organization Administrator Group.

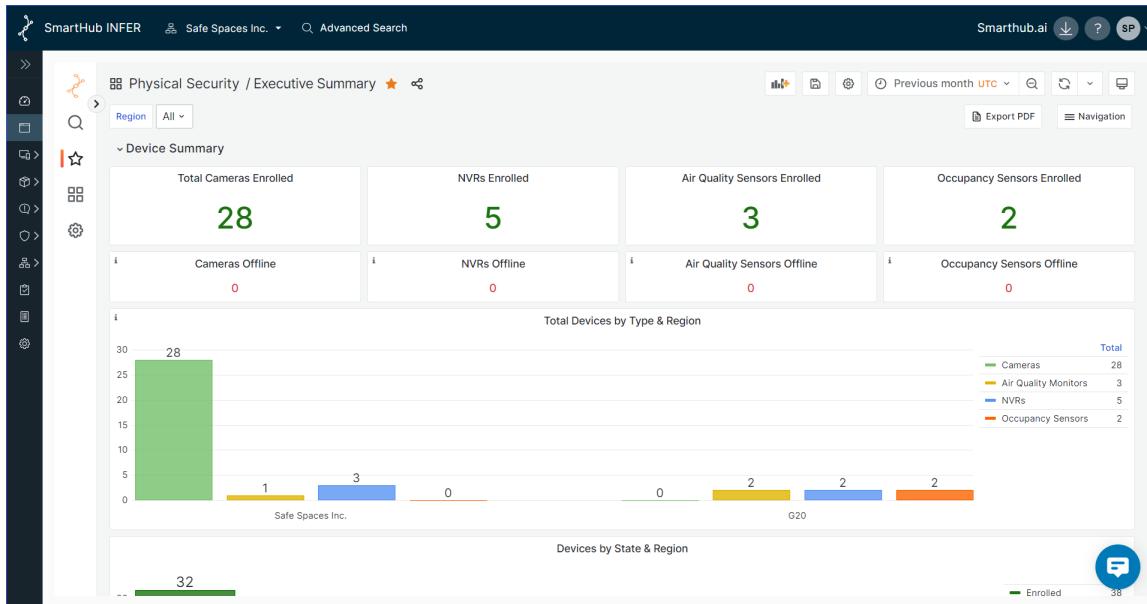


For more information see "Roles and Permissions" on page 3.

1. From the INFER™ Console, go to **Insights**. The default homepage, **Executive Summary** page appears as shown below:



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



3. Under **Device Summary**, as you scroll down, you can see various clickable panels showing the devices' 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. Devices Need Attention
4. Alternatively, you can also click **Navigation** on the top right to list and access all dashboards available for your organization, as shown below:



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:

Key Network Settings for Cameras								
Name	IP Address	SSH Enabled	RTSP	Enabled	HTTP Enabled	HTTPS Enabled		
Axis Q3515 LV IND BLR SH 192.168.29.4	192.168.29.4	no	yes	<input checked="" type="radio"/> View	<input type="checkbox"/> Edit	<input type="checkbox"/> Share	<input type="checkbox"/> Explore	<input type="checkbox"/> Inspect
Axis-Physec-Lab	192.168.29.4	yes	yes	<input type="radio"/> View	<input checked="" type="checkbox"/> Edit	<input checked="" type="checkbox"/> Share	<input checked="" type="checkbox"/> Explore	<input checked="" type="checkbox"/> Inspect
Dell Demo May 30th	192.168.29.4	no	yes	<input type="radio"/> View	<input checked="" type="checkbox"/> Edit	<input checked="" type="checkbox"/> Share	<input checked="" type="checkbox"/> Explore	<input checked="" type="checkbox"/> Inspect
GP-Test-Camera March 15th	10.42.0.121	no	yes	<input type="radio"/> View	<input checked="" type="checkbox"/> Edit	<input checked="" type="checkbox"/> Share	<input checked="" type="checkbox"/> Explore	<input checked="" type="checkbox"/> Inspect
IND-BLR-3F_ENTRY ROOM	115.31.187.247	no	yes	<input type="radio"/> View	<input checked="" type="checkbox"/> Edit	<input checked="" type="checkbox"/> Share	<input checked="" type="checkbox"/> Explore	<input checked="" type="checkbox"/> Inspect
IND-BLR-3F_IDF ROOM	75.37.239.39	no	yes	<input type="radio"/> View	<input checked="" type="checkbox"/> Edit	<input checked="" type="checkbox"/> Share	<input checked="" type="checkbox"/> Explore	<input checked="" type="checkbox"/> Inspect

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



The screenshot shows a SmartHub.ai dashboard titled "Physical Security / Cameras". The top navigation bar includes filters for Region, Country, City, Building, Floor, Camera, and a "Navigation" button. The main content area is titled "Key Network Settings for Cameras" and displays a table with the following columns: Name, IP Address, SSH Enabled, RTSP Enabled, FTP Enabled, HTTP Enabled, and HTTPS Enabled. The table lists 16 cameras with their respective details.

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

4.1.1 Exporting to PDF

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

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

4.2 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 to zoom out the time range.



The dashboard and panel time controls have a common Console.

3. **Refresh dashboard:** Click 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  to display the dashboard on a large screen such as a TV or a kiosk.

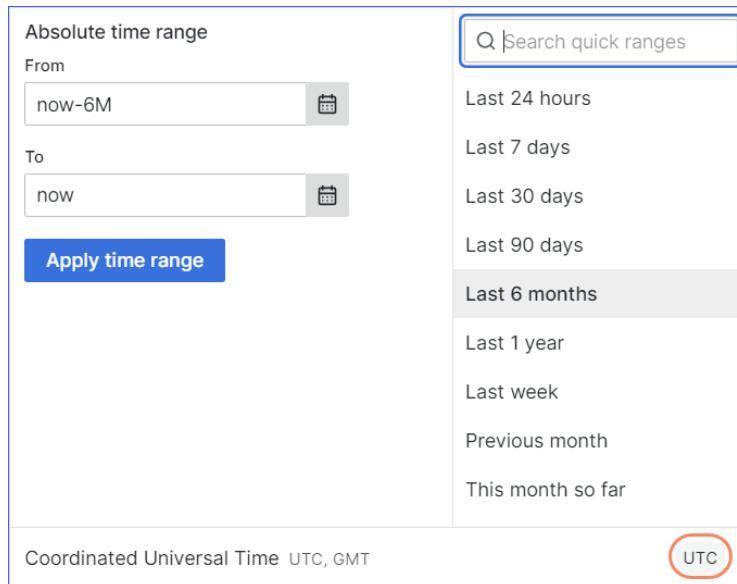


View mode hides irrelevant information such as navigation menus.

5. **Starred dashboards:** Starred dashboards help you remember to look at them later within Insights. You can mark your favorite dashboards by clicking  against any listed dashboard and change its color to .

4.2.1 Setting Absolute time range

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



Absolute time range

From: now-6M To: now

Apply time range

Search quick ranges

- 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.



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

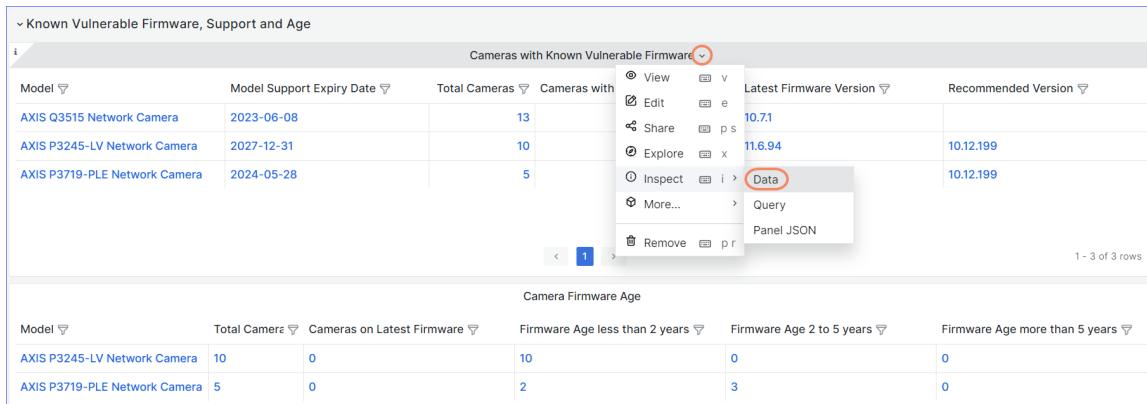
4. Click **Apply time range**.

4.3 Downloading Data from Table Panels

The table panel has 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

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

Camera Firmware Age					
Model	Total Camera	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

A Model	A Model Suppor	■ Total Camer	■ Cameras with	A I
AXIS Q3515 Network Camera	2023-06-08	13	7	10.7
AXIS P3245-LV Network Camera	2027-12-31	10	8	11.6
AXIS P3719-PLE Network Camera	2024-05-28	5	5	11.6

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

5 Spaces

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

Spaces in INFER™ typically refer to the environments or contexts where IoT devices are deployed. These spaces can vary widely, from homes and offices to industrial settings and smart cities. The concept of Space involves integrating IoT devices into specific spaces to gather data, enable automation, and enhance overall efficiency.

5.1 Creating Spaces

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:

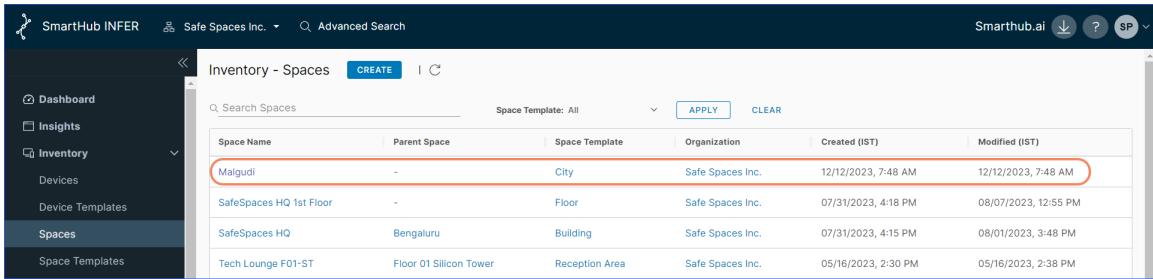


For more information see "Roles and Permissions" on page 3.

1. From the INFER™ Console, go to **Spaces**. The **Inventory - Spaces** page appears.
2. Click **CREATE**. The **Create Space** wizard appears.
3. Under **Space Template**, select the desired template from the drop-down.
4. Under **Display Name**, enter the desired name for the space template you are creating.
5. Click **NEXT**.
6. Under **Space Attributes**, click  to modify values of default attributes.
7. Click **+ Add** and under **Name**, enter the new attribute's name.
8. Under **Value**, from the drop-down, 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, and the following action confirmation message appears:

 Space created successfully

10. You can now view your space in the **Inventory - Spaces** page as shown below:



Space Name	Parent Space	Space Template	Organization	Created (IST)	Modified (IST)
Malgudi	-	City	Safe Spaces Inc.	12/12/2023, 7:48 AM	12/12/2023, 7:48 AM
SafeSpaces HQ 1st Floor	-	Floor	Safe Spaces Inc.	07/31/2023, 4:18 PM	08/07/2023, 12:55 PM
SafeSpaces HQ	Bengaluru	Building	Safe Spaces Inc.	07/31/2023, 4:15 PM	08/01/2023, 3:48 PM
Tech Lounge F01-ST	Floor 01 Silicon Tower	Reception Area	Safe Spaces Inc.	05/16/2023, 2:30 PM	05/16/2023, 2:38 PM

5.2 Editing Spaces

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:



For more information see ""Roles and Permissions" on page 3"

1. From the INFER™ Console, go to **Spaces**. The **Inventory - Spaces** page appears.
2. From the listed spaces, click the space you desire to edit.
3. Under **Actions**, from the drop-down, click **Edit**.
4. The **Edit Space** wizard appears. Here, update the **Space Template**, **Display Name**, **Space Attributes** and click **NEXT**.
5. Under **Review**, review the information and click **SAVE**. You have successfully edited a space, and the following action confirmation message appears:

 Space updated successfully

5.3 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.

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:



For more information see ""Roles and Permissions" on page 3"

1. From the INFER™ dashboard Console, go to **Spaces > Inventory - 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:

Space Name	Id
SafeSpaces HQ	00259ed5-621b-404c-a352-3ce2b
SafeSpaces HQ 1st Floor	24ca4d88-496e-48e6-97cc-b5893
Tech Lounge F01-ST	54b33c30-45c6-4adc-8b2d-f19bd
Code Cuisine F02-ST	b8cff4cb-cdda-43a8-8dac-dc1a25
Solution Space F02-ST	56d5f9af-8933-440e-adb8-256fda
Robotics Den F02-ST	4802e998-025b-422d-a682-f45a0
Cyber Hive F01-ST	26a36b0d-3c46-4532-86f6-e4796
Data Oasis F01-ST	7172bded-64e6-4959-940c-a3412
Floor 02 Silicon Tower	3a7c4e72-dd0b-4bef-9077-20aa11
Floor 01 Silicon Tower	ef7a8522-62cb-4804-a0ff-d0f2da5
Silicon Tower	7506e827-7f4e-4fd6-917b-5d4126
Palo Alto	cc111acc-690c-4d08-9613-9c6077

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, and the following action confirmation message appears:



5.4 Bulk Assign Spaces to Devices

You can select multiple devices and assign to multiple spaces.

1. From the INFER™ dashboard Console, go to **Inventory > Inventory - Devices**.
2. Select the checkboxes of your desired devices for which you want to assign spaces.



Each page lists 20 devices. If no device check boxes are selected, INFER auto-selects devices across all list pages.

3. Go to **Actions** drop-down > **Bulk Assign Space**. The **Bulk Assign Space** pop-up appears as shown below:



Bulk Assign Space

X

Total 4 Device(s) selected, Assigning the Space to the device(s) using a Spreadsheet is done in three steps

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

[DOWNLOAD SPREADSHEET](#)

Step 2 - Edit Spreadsheet

In the downloaded Spreadsheet,

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

Step 3 - Upload the updated Spreadsheet

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

[ASSIGN](#)

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



- **Device Id** (column A) and **Space Id** (column E) are kept hidden on purpose.
- Do not modify any columns except **Space**.
- Devices in **Green** background are already assigned with spaces. However, you can reassign them to different spaces.
- Do not delete/edit existing column headers.

6. If you attempt to modify existing column headers, the following error message appears:



The cell or chart you're trying to change is on a protected sheet. To make a change, unprotect the sheet. You might be requested to enter a password.

OK

5.4.1 Modifying Spaces

7. Under **Space** column, click against any device to pull the drop-down and select desired space.
8. After you complete assigning spaces to devices, save the file to disk in its original **XLSX** format.
9. 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 X

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

ASSIGN

10. Click **ASSIGN** to bulk assign spaces to devices, and the following action confirmation message appears:

Successfully assigned Space(s) to Device(s) X

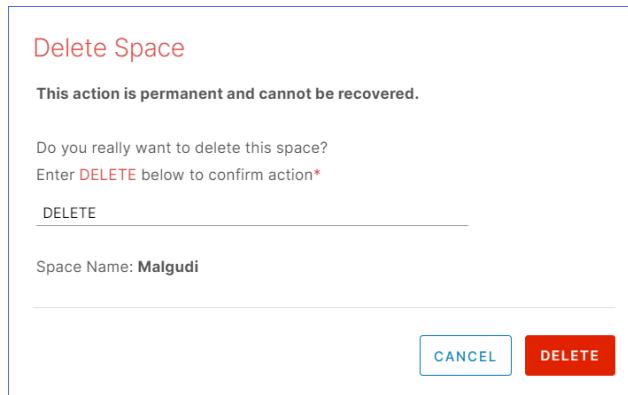
5.5 Deleting Spaces

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:

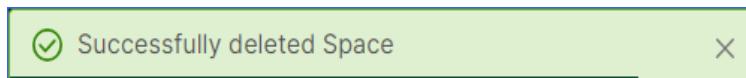


For more information see ""Roles and Permissions" on page 3"

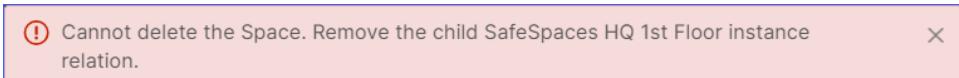
1. From the INFER™ Console, go to **Spaces**. The **Inventory - Spaces** page appears.
2. From the listed spaces, click the space you desire to delete.
3. Under **Actions**, from the drop-down, click **Delete**.
4. The **Delete Space** pop-up appears as shown below:



5. Enter **DELETE** in the text area, and click **DELETE**. You have successfully deleted a space, and the following action confirmation message appears:



6. In case the selected space is already associated with a child space, the following error message appears:



6 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.

6.1 Smart Spaces

Smart spaces refer to environments that are equipped with various IoT devices, sensors, and technologies to collect, analyze, and act on data for the purpose of optimizing 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.

6.2 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 underutilized 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.

6.3 What is a Space Template?

A space template in INFER™ takes stock of a space's location, dimensions, and actions by collecting its attributes from your space management system in use as per the defined data model. It serves as a predefined structure or blueprint that defines the characteristics, functionalities, and behaviors for multiple spaces with similar features and configurations to stay connected.

6.4 Creating a Space Template

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



For more information see "Roles and Permissions" on page 3.

1. From the INFER™ Console, go to **Space Templates**. The **Inventory - Space Templates** 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, choose the desired attribute type.



- 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 while creating a space.

Create Space Template

- 1 Details
- 2 Attributes**
- 3 Review

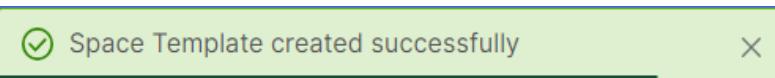
Attributes

Space Template Attributes

Name	Type	Value	Edit
Area-Conference Room	STRING	3000 Sqft	
MAX_OCCUPANCY_THRESHOLD	CONSTANTS	20, 30, 40, 50	
+ 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, and the following action confirmation message appears:



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

The screenshot shows the SmartHub INFER interface. On the left, there is a dark sidebar with various navigation options like Dashboard, Insights, Inventory, Space Templates, etc. The 'Space Templates' option is currently selected. The main area is titled 'Inventory - Space Templates' and contains a table of space templates. The table has columns for 'Space Template Name', 'Description', 'Parent Templates', 'Organization', 'Created', and 'Modified'. The first row shows 'SafeSpaces Building HQ' with a description of 'Bangalore-Kadubheesanhalli', no parent template, and it was created on 07/31/2023 at 11:33 AM. Other rows include 'Canteen Area', 'Reception Area', 'Room', 'Floor', 'Building', 'City', and 'Country'. A blue oval highlights the 'Parent Templates' column for the first row. At the bottom of the table, it says '1 - 8 of 8 Space Templates'.

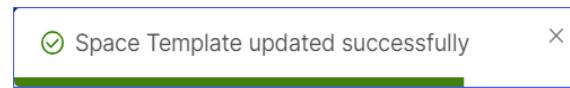
6.5 Editing a Space Template

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:



For more information see ""Roles and Permissions" on page 3"

1. From the INFER™ Console, go to **Space Templates**. The **Inventory - Space Templates** page is displayed.
2. From the listed templates, click the template you desire to edit.
3. Under **Actions**, from the drop-down, 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, and the following action confirmation message appears:



6.6 Assigning a Parent Template

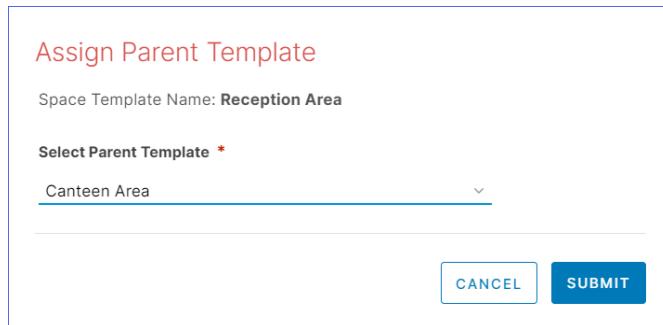
To assign a parent template in INFER™, you must have the EDIT_SPACE_TEMPLATE permission associated with the Organization Administrator Group, and perform the following steps:



For more information see ""Roles and Permissions" on page 3"

1. From the INFER™ Console, go to **Space Templates**. The **Inventory - Space Templates** page is displayed.
2. From the listed templates, click the template you desire to assign a parent template.
3. Next, 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:



The form has a title "Assign Parent Template". It contains a field "Space Template Name: Reception Area". Below it is a section "Select Parent Template *". A dropdown menu is open, showing "Canteen Area" as the selected option. At the bottom are two buttons: "CANCEL" and "SUBMIT".

5. Under **Select Parent Template**, use the drop-down to select your desired parent template.
6. Click **SUBMIT**. You have successfully assigned a parent template, and the following action confirmation message appears:



6.7 Cloning a Space Template

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

Cloning an 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.

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:



For more information see ""Roles and Permissions" on page 3"

1. From the INFER™ dashboard Console, go to **Spaces > Inventory - Spaces**.
2. From the listed templates, click the template you desire 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** to add new attributes, and click **NEXT**.
 7. Under **Review**, review the information and click **SAVE**. You have successfully cloned a space template, and the following action confirmation message appears:



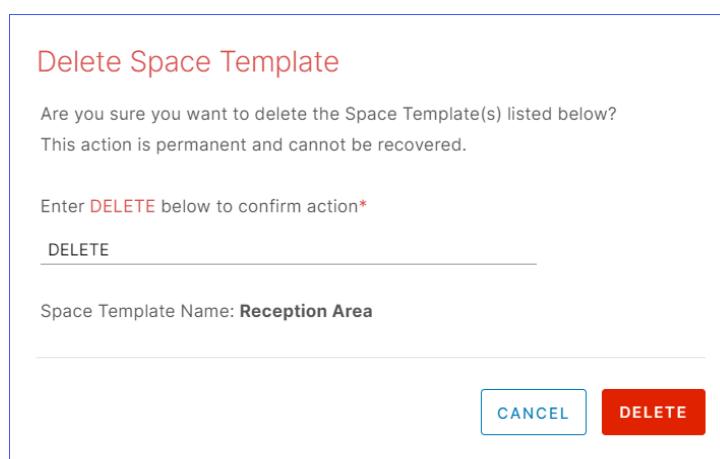
6.8 Deleting a Space Template

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:



For more information see ""Roles and Permissions" on page 3"

1. From the INFER™ dashboard Console, go 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** pop-up appears as shown below:

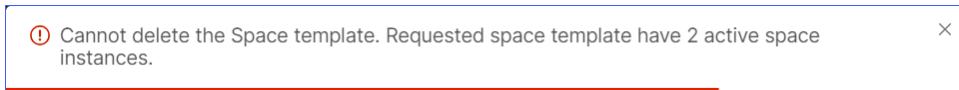
A modal dialog box titled "Delete Space Template" in red at the top center. Below the title, a message asks, "Are you sure you want to delete the Space Template(s) listed below? This action is permanent and cannot be recovered." A text input field below the message prompts the user to "Enter **DELETE** below to confirm action*". A horizontal line with the word "DELETE" typed into it follows. At the bottom of the dialog, the text "Space Template Name: Reception Area" is displayed above two buttons: "CANCEL" in a light blue box and "DELETE" in a red box.



-
5. Enter **DELETE** in the text area, and click **DELETE**. You have successfully deleted a space, and the following action confirmation message appears:



6. In case the selected space is already associated with a child space, the following error message appears:



7 Working with Device Templates

This chapter explains devices, device templates, and the steps to create and edit devices and device templates.

A device template takes stock of the device's behaviors and actions by collecting system properties from the device, 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 devices with similar features and configurations to stay connected.

7.1 What is a Device?

A device in INFER™ refers to an entity which can be given an identity, be managed, stay connected to the internet and is capable of collecting, transmitting, and receiving data. Such devices are embedded with sensors, software, and network connectivity, allowing them to interact with their surroundings, other devices, and users.

There are 2 types of devices:

1. **Gateway:** A device entity in which an [Agent](#) can be run directly, giving you greater control and which also allows you to talk to other devices 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 devices. 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.



A gateway is designed to support a maximum of 400 devices, configured as a soft limit.

2. **Thing:** A very light weight device 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 device, wait for the outcome of the command, and take it back to the user who gave that command.



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

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

7.2 What is a Device Template?

When we consider IoT devices in an enterprise, it is in scale amounting to hundreds of thousands of devices. It is practically impossible to deal with each device one at a time. This situation therefore calls for an ability to deal with thousands of devices at a time. To do so, we give them a generic model which we call a **Device Template**.

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

There are two types of templates in INFER™:

1. Gateway type
2. Thing type

7.3 What are Device Properties?

The device template contains the following properties:

- System Properties
- Custom Properties

7.3.1 System Properties

These are Properties of the device itself collected automatically by the Agent. It includes device 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 device itself. You can query these properties using **Advanced Search**.

7.3.2 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 device. These properties can be associated with a device's golden configuration template settings, or warranty information. By default, every new devices gets this data. Once onboarded, every device 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 devices.

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

The device template carries commands which specify what actions which the device can support. Connected templates express the relationship between gateway template and Programmable Logic Controller (PLC) and.... The structure is well defined and managed.

7.4 What are Metrics?

Both **Gateway** and **Thing** templates support the Agent's collection of Metrics or telemetry data from the devices specified by the INFER™ Server. This numeric, boolean, and string data types are also called time-series data as its values keep changing very frequently. You can configure metric keys such as **Name**, **Value Type**, and **Display Unit**. The metric value type is pre-defined in the device template and is validated on the Agent.

7.5 INFER™ Agent Daemon

The INFER™ Agent is a gateway container or a virtual machine that allow its adapters to talk to the devices, 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 device in its own language to make things work.

Whether the devices are on IP, Modbus, Lonworks, or BACnet, their adapters'll talk to them, collect the 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'll embed 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. That gets all the data into the Server having a rich REST API.

7.5.1 What is an Adapter?

The adapter is the software piece that bridges the protocol gaps between the device and the Server. The adapter and device template work together as tightly coupled entities. If the device 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 device template.

7.5.2 Connected Device Templates

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

7.5.3 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

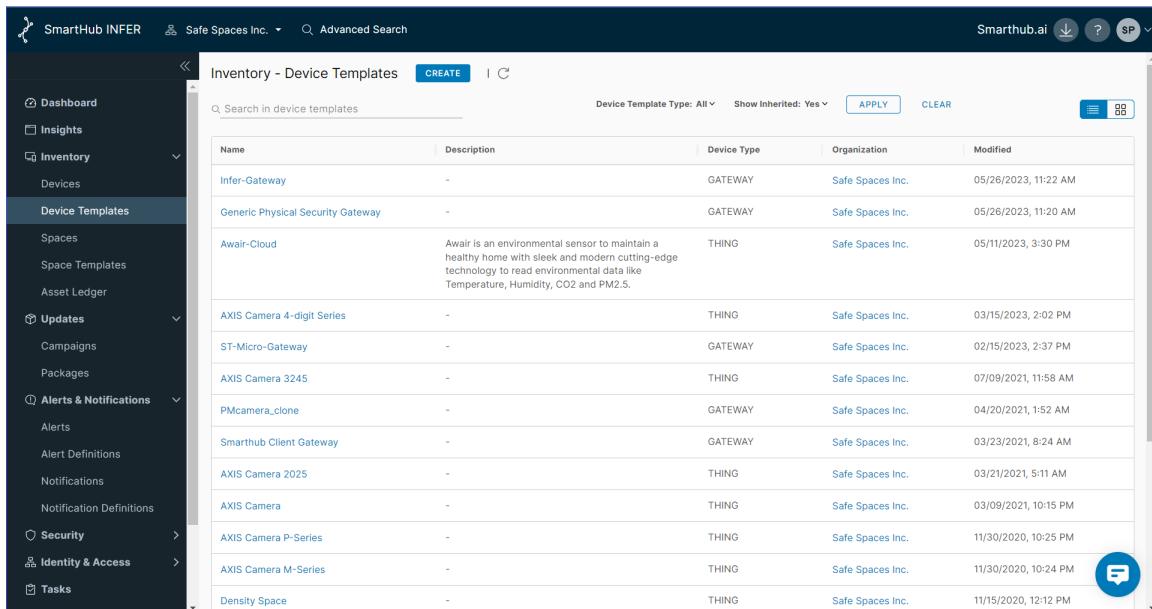
4. Reboot

5. SSH

For more information about these commands, see the [Creating a Device Template](#) section below.

A device created from a template receives the default configuration of the template. The device template helps in creating a simplified process for registering new devices.

A device can have a restricted list of Thing devices with a specified template. You can create a device based on the list of available Thing templates. To connect a Thing device, ensure that the Thing template is a part of the parent gateway template.



Name	Description	Device Type	Organization	Modified
Infer-Gateway	-	GATEWAY	Safe Spaces Inc.	05/26/2023, 11:22 AM
Generic Physical Security Gateway	-	GATEWAY	Safe Spaces Inc.	05/26/2023, 11:20 AM
Awair-Cloud	Awair is an environmental sensor to maintain a healthy home with sleek and modern cutting-edge technology to read environmental data like Temperature, Humidity, CO2 and PM2.5.	THING	Safe Spaces Inc.	05/11/2023, 3:30 PM
AXIS Camera 4-digit Series	-	THING	Safe Spaces Inc.	03/15/2023, 2:02 PM
ST-Micro-Gateway	-	GATEWAY	Safe Spaces Inc.	02/15/2023, 2:37 PM
AXIS Camera 3245	-	THING	Safe Spaces Inc.	07/09/2021, 11:58 AM
PMcamera_clone	-	GATEWAY	Safe Spaces Inc.	04/20/2021, 1:52 AM
Smarthub Client Gateway	-	GATEWAY	Safe Spaces Inc.	03/23/2021, 8:24 AM
AXIS Camera 2025	-	THING	Safe Spaces Inc.	03/21/2021, 5:11 AM
AXIS Camera	-	THING	Safe Spaces Inc.	03/09/2021, 10:15 PM
AXIS Camera P-Series	-	THING	Safe Spaces Inc.	11/30/2020, 10:25 PM
AXIS Camera M-Series	-	THING	Safe Spaces Inc.	11/30/2020, 10:24 PM
Density Space	-	THING	Safe Spaces Inc.	11/15/2020, 12:12 PM

To view more details of a device template, click the name of the desired device template in the Device Templates page as shown above.

7.5.4 Creating a Device Template

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



For more information see "Roles and Permissions" on page 3.

1. From the INFER™ Console, go to **Device Templates**. The **Inventory - Device Templates** page is displayed.
2. Click **CREATE**. The **Create Device 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 Device Type**, choose between **Gateway** and **Thing** from the drop-down.
6. Under **Description**, enter a brief description of the device 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 **System Properties**, view the registered device's system properties that are automatically collected by the Agent or its User client node and sent to the INFER™ Server.



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

10. Click to modify property parameters like the **Name**, and **Description**.
11. Toggle the **Sensitive Property** switch for adding an extra layer of protection to a property, and click **DONE**.
12. Click **CANCEL** to discard property modifications.
13. Click  to delete the property.
14. To add a new system property, scroll down and click . Enter the parameters and click **DONE**.
15. Next, scroll down to view **Custom Properties**.

Entered by the administrator, **Custom Properties** are the default properties associated with all the devices attached to this template. These properties are used for querying information or for sending configuration files to the devices.

However, unlike **System Properties**, these properties are not collected from the device and can be edited on the Server.

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



The Metric **Name** and **Value Type** collected from the device must match the **Allowed 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 device, perform the next steps. However, if you have selected **Thing** as your device, go to the last step.

22. Click **NEXT**.
23. Under **Connected Device Templates**, you can edit or delete the thing device template that is connected to this device.



Only those devices that belong to the connected templates list can be associated with this device template.

24. To add a device template, click **+ Add**.
25. Under **Template**, select the desired template from the drop-down and click **DONE**.
26. Click **Next**.



-
27. Under **Commands**, to add a command, click .
 28. Under **Type** from the drop-down, select the command type you want to run on your device:
 - I. **Client Command** - Set a command to communicate with the connected devices 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 devices.
 - II. **Custom Command** - Set a custom command. For example, set a command to configure the IP address of the device 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.
 - III. **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.
 - IV. **Reboot** - Set a command to reboot the device.
 - V. **SSH** - Set a command to enable or disable SSH on the device.
 29. Under **Description**, enter a brief description of the command you are creating, and click **DONE**.
 30. Click **NEXT**.
 31. Under **Enrollment Provider**, configure the enrollment provider settings used for creating device credentials. These credentials are used for onboarding devices securely.
 32. Under **Provider Type**, select the desired enrollment provider from the drop-down. This creates a single use device credential with signature and expiry time verification.

-
33. Under **Provider Config > Identity Key**, specify the key whose value will be presented by this device during onboarding.
 34. Click **NEXT**.
 35. Under **Settings > Agent Settings**,
 - I. Under **Log Level**, use the drop-down to set the logging level for collecting **Error, Warning, Info** or **Debug** Agent logs on a device .
 - II. Under **Maximum Number of Clients**, set the maximum number of SDK clients that can communicate through the Agent with the INFER™ Server.
 - III. 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 is displayed.
 - IV. Under **Metrics Interval (seconds)**, set the time interval between 60 and 43200 seconds for transmitting metrics from the Agent to the INFER™ Server.



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 is displayed.

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



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 is displayed.



-
- VI. Under **Network Bandwidth (bytes / second)**, set the maximum network bandwidth allowed on the device for the Agent. The data rate is in Bytes per second (B/s). The value "0" denotes unlimited network bandwidth. Configure the network bandwidth cap on the device for the Agent (in bytes per second).
 - VII. Under **Forward Proxy**, click to enter the **Server**, **Port** and user credentials, and click **NEXT**.
 - VIII. Under **Network Bandwidth (bytes / second)**, set the maximum network bandwidth allowed on the device for the Agent. The data rate is in Bytes per second (B/s). The value "0" denotes unlimited network bandwidth. Configure the network bandwidth cap on the device for the Agent (in bytes per second).
 - IX. Under **Forward Proxy**, click to enter the **Server**, **Port** and user credentials, and click **NEXT**.

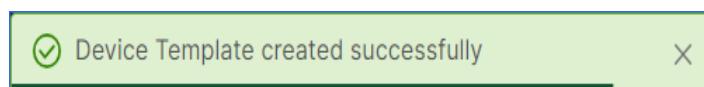
You can add multiple HTTP Proxy settings. These proxy settings details are stored in the INFER™ Agent configuration file. The INFER™ Agent uses these proxy settings to connect to the Server for enrolling a gateway.



The proxy settings details are then sent to the gateway while enrolling a device 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.

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.

- 30. Under **Review**, review the device template information you entered and click **SAVE**. You have successfully created a device template, and the following action confirmation message appears:



- 31. You can now view your device template in the **Devices - Device Templates** page.

7.6 Editing a Device Template

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



For more information see ""Roles and Permissions" on page 3"

1. From the INFER™ dashboard Console, go to **Inventory > Device Templates**.
2. From the listed templates, click the template you desire to edit. The following tabs appear as highlighted below:

Name	Id
SafeSpaces_Gateway	b29cb2e2-ef74
Infer-Gateway	53d9a25c-a5e5
Generic Physical Security Gateway	c8a24167-86aa
Awair-Cloud	ea2346c9-8767
AXIS Camera 4-digit Series	353869f2-a798
ST-Micro-Gateway	b3c379b7-b875
AXIS Camera 3245	09c56936-ac94
PMcamera_clone	7217733d-0853
Smarthub Client Gateway	47838513-e59c
AXIS Camera 2025	8c62409b-ebdc

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



You cannot edit the template name and device type.

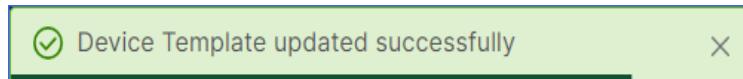
5. Under **System Properties**, click against a property to edit that property, make required changes and click **DONE**.



If this device 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 icon.
 7. To add a new system property, click and enter the property name, and click **DONE**.
 8. Under **Review**, review the device template information you entered and click **SAVE**. You have successfully edited a device template, and the following action confirmation message appears:



7.6.1 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 endpoint. 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 Device Template** wizard, proceed to the **Commands** page.
2. Under **Commands**, click **+ Add**.
3. Under **Type**, select **Custom Command** from the drop-down.
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.

8 Onboarding Gateways

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

8.1 What is a Gateway?

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

Listed below are the functions of a gateway:

- **Protocol Translation**: Gateway devices 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 devices and INFER™.
- **Connectivity Management**: Gateways maintain the connectivity between IoT devices and INFER™. They handle tasks like device registration, authentication, and network configuration, ensuring reliable and secure communication.
- **Data Aggregation and Pre-processing**: Gateways collect data from multiple devices 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 devices before allowing data transmission to the central server or cloud.
- **Device Management and Firmware Updates**: Gateways facilitate device management tasks, including remote configuration, monitoring, and firmware



updates. They provide a centralized control point for managing a fleet of IoT devices, 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 devices.

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



The definition is in the template, and its implementation is done in the adapter. Therefore, if the device 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 a device template as explained in "Creating a Device Template" on page 54.
2. "Working with INFER™ Agent" on page 84.
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 device 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 device 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 devices 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 device and use it to authenticate the device's identity.



- TPM-based enrollment is hardware-based and built into the device.
- Certificate-based enrollment is a file distributed into the



devices 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 devices 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 device 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 device'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 device on for the 1st time along with network connection, he can log in via his mobile application and whitelist this device. So, besides matching the device's serial number, the Whitelisting process in device enrollment gives the extra protection layer to the device.
- 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.

8.2 Onboarding a Gateway using Basic Authentication

Before you onboard a gateway using the basic authentication method, all the line items in the checklist below must be fulfilled:

- I. Ensure that you have the user name and password of the user in the organization where you want to enroll the device. (*username* and *password*)
- II. If the user has an account in multiple organizations, then ensure that you have the **Domain Name** for the Organization where the device is to be enrolled. (*user-orgdomain-name*)
- III. You must have created a device template with **Basic Enrollment** as the **Provider Type**, and it must be available on INFER™ Console. (*template*)
- IV. By default, the Device will be enrolled in the Organization where the user's account exists. However, if you wish to enroll the Device in a sub-organization, then ensure that you have the **Organization ID** of the sub-org. (*device-org-id*)
- V. You must have installed the Agent on your gateway.
- VI. You must know the name that you want to assign to your gateway in INFER Console. (*name*)

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

1. From the INFER™ Console, go the **Inventory> Device Templates**.
2. Identify the device template to be associated with your gateway.
3. Log in to your gateway and change the directory to
 - **For Linux:** /opt/smarthub/iotc-agent/bin
 - **For Windows:** C:/ProgramFiles/SmartHub/iotc-agent/bin

Run the following command:

```

./DefaultClient enroll --auth-type=BASIC [--device-org-
id=<org domain id>]

--template=<template name> --name=<gateway name>

[--user-org-domain-name=<organization domain
name>]

--username=<user name> [ --
password=<prompt|file:<path>> ]

```



- If you are providing a file as input for the password, ensure that the file is accessible by the Default Client.
 - 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 device ID to it.
 5. To verify that the gateway is enrolled, go to the INFER™ Console and click the **Devices** tab. You can see that the gateway is listed in the **Devices - All Devices** page and its status must be **ENROLLED**.

8.3 Onboarding a Gateway using Token-Based Authentication

Before you onboard a gateway using the token-based authentication method, all the line items in the checklist below must be fulfilled:

- I. You must have the **CREATE DEVICE** permission to perform this operation.
- II. You must have created a device template with **Token-based** as the **Provider Type**, and it must be available on the INFER™ Console.
- III. You must have installed the Agent on your gateway.
- IV. You must know the name you are going to assign to your gateway in the INFER™ Console.

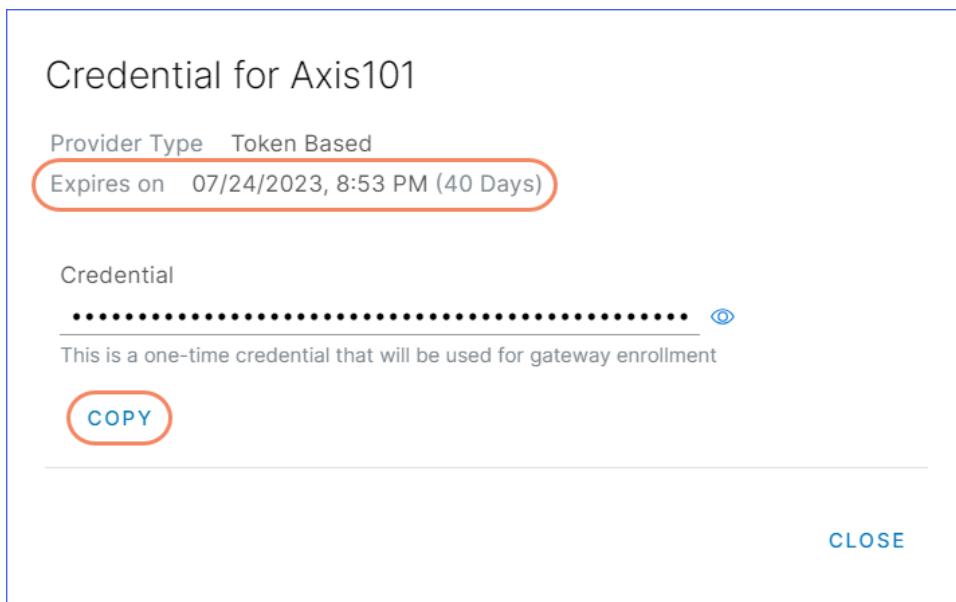
To onboard a gateway using the token-based authentication method, perform the following steps:

1. From the INFER™ Console, go the **Inventory > Devices > REGISTER > Gateway**. The **Register Gateway** pop-up is displayed.
2. Under **Device Template**, from the drop-down, select your desired template that has Token-based Authentication enabled to associate with your gateway.
3. Under **Device Name**, enter your desired gateway name.
4. Click **REGISTER**. You have successfully registered your gateway and the following action confirmation message appears:

 Device created successfully

X

5. Now, your newly registered gateway appears listed in the **Devices - All Devices** page.
6. Next, create a credential to enroll your gateway. To do so, from the **Devices - All Devices** page, click the gateway that you just registered.
7. Click the **Actions** drop-down and select **Create Gateway Credentials**. Click **CREATE**. The following pop-up appears as shown below:



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

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



For a successful enrollment, the response must be 0.

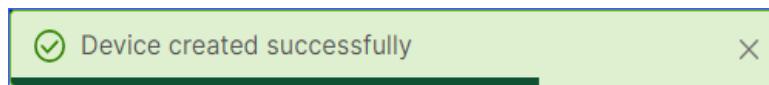
8.4 Onboarding a Gateway using Property-based Authentication

Before you onboard a gateway using the property-based authentication method, all the line items in the checklist below must be fulfilled:

- I. You must have the **CREATE DEVICE** permission to perform this operation.
- II. You must have installed the Agent on your gateway.
- III. You must have created a device template with **Property-based** set as **Provider Type**, and it must be available on the INFER Console.
- IV. You must know the name that you want to assign to your gateway in the INFER Console.

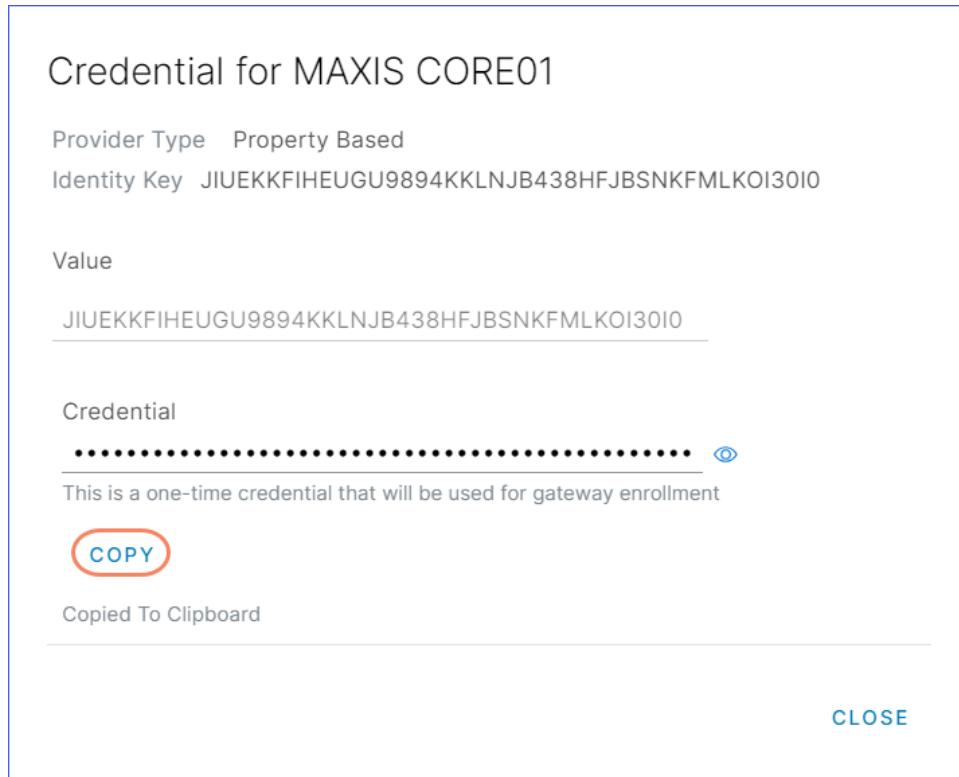
To onboard a gateway using the property-based authentication method, perform the following steps:

1. From the INFER™Console, go the **Inventory > Devices > REGISTER > Gateway**. The **Register Gateway** pop-up is displayed.
2. Under **Device Template**, from the drop-down, select your desired template that has Token-Based Authentication enabled to associate with your gateway.
3. Under **Device Name**, enter your desired gateway name.
4. Click **REGISTER**. You have successfully registered your gateway and the following action confirmation message appears:



5. Alternately, your newly registered gateway appears listed in the **Devices - All Devices** page.
6. Next, you need to create a credential to enroll your gateway. To do so, from the **Devices - All Devices** page, click the gateway that you just registered.

7. Click the **Actions** drop-down and select **Create Gateway Credentials**. Click **CREATE**. The following pop-up appears as shown below:



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

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



For a successful enrollment, the response must be 0.

8.5 Onboarding a Gateway using TPM-based Authentication

Before you onboard a gateway using the Trusted Platform Module-based authentication method, all the line items in the checklist below must be fulfilled:

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

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

The output must display the following response:

```
SmartHub secured.
```

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

- If `SmartHub secured` is not displayed, 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'
```

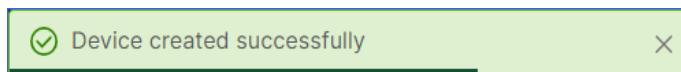
- To run every time your gateway starts, add the following commands in a run script:

```
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 device /dev/tpmrm0.
```

- V. You must have the **CREATE DEVICE** permission to perform this operation.
- VI. You must have created a device template with **TPM Based** as the **Provider Type**, and it must be available on the INFER™ Console.
- VII. You must know the name that you want to assign to your gateway in the INFER™ Console.

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

1. From the INFER™ Console, go the **Inventory > Devices > REGISTER > Gateway**. The **Register Gateway** pop-up is displayed.
2. Under **Device Template**, from the drop-down, select your desired template that has TPM-based Authentication enabled to associate with your gateway.
3. Under **Device Name**, enter your desired gateway name.
4. Click **REGISTER**. You have successfully registered your gateway and the following action confirmation message appears:



5. Now, your newly registered gateway appears listed in the **Devices - All Devices page**.

6. Next, you need to create a credential to enroll your gateway. To do so, from the **Devices - All Devices** page, click the gateway that you just registered.
7. 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:/ProgramFiles/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:/ProgramFiles/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.

8.6 Onboarding a Gateway using Zero Touch Enrollment

Before you onboard a gateway using the Zero Touch Enrollment method, all the line items in the checklist below must be fulfilled:

- I. You must have the **CREATE DEVICE** and **ZERO TOUCH ENROLLMENT** permissions to perform this operation.
- II. You must have created a device template with **Zero Touch Enrollment** as the **Provider Type**, and it must be available on the INFER™ Console.
- III. The gateway must be a Dell gateway running Ubuntu Server and must be Zero Touch Enrollment enabled.
- IV. You must have created a CSV file that contains the list of devices to enroll, along with the following columns:
 - a. Hardware Id (mandatory)
 - b. Model Number (optional)
 - c. Property Value (optional)

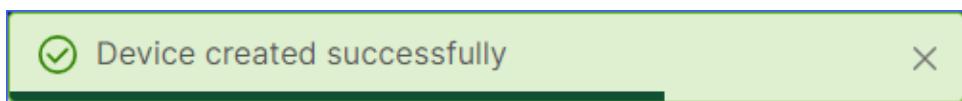
To onboard a gateway using the Zero Touch Enrollment method, perform the following steps:

1. From the INFER™ Console, go to the **Inventory > Devices > REGISTER > Gateway**. The **Register Gateway** pop-up is displayed.
2. Under **Device Template**, from the drop-down, select your desired template that has Zero Touch Enrollment enabled to associate with your gateway.



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

3. Under **Device Name**, enter your desired gateway name.
4. Click **REGISTER**. You have successfully registered your gateway and the following action confirmation message appears:



-
5. Click **Upload** to upload the CSV file that contains a list of Hardware IDs of your gateways.
 - I. The first row is reserved for the property name.
 - II. The **HardwareId** field is mandatory.
 - III. The **Model Number** and **Property value** fields are optional.
 - IV. Any values and names provided after the first column are displayed as custom properties on the registered gateways.

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

6. Click **REGISTER**.

8.7 Whitelisting a Device

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 device template that has the **Requires Whitelisting** option enabled, select **Whitelist** from the **Actions** drop-down to enroll the gateway.

8.8 Registering Multiple Devices using CLI

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

Ensure that you create a JSON file with the device template name, list of devices, 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 devices 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 device commands that enable you register your devices in bulk:

```
a01:iot-cli xyz$ ./bin/darwin_amd64/package-cli devices  
Manage devices 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 "./iot-  
                                cli.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-cl i xyz$ ./package-cl i 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-bfcf-  
b77febbf3a56 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 devices are listed in the **Inventory - Devices** page of the INFER™ Console.

8.9 Registering Multiple Gateways

To register Gateways in bulk, perform the following steps:

1. From the INFER™ Console, go to **Devices > Inventory Devices > Register > Multiple Gateways**. The **Bulk Register Gateways** wizard appears as shown below:

<p>Bulk Register Gateways</p> <ul style="list-style-type: none"> 1 Device Template 2 Upload Gateway Details 3 Register Gateways 4 Summary 	<p>Select Device Template</p> <p>Select the Device Template for which you wish to Register Gateways</p> <p>Device Template</p> <p>Select Device Template</p> <p style="text-align: right;">CANCEL NEXT</p>
---	--

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



Only one device template can be used to register multiple gateways at a time.

3. Click **NEXT**.
4. As per the device 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 device identities to all the gateways being enrolled. For more information, see "Onboarding a Gateway using Token-Based Authentication" on page 68



- For **Property Based Enrollment**, toggle the **Setup Gateway Credentials** switch to toggle option.



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

5. Click **NEXT**.
6. Under **Upload Gateway Details**, download the CSV template file .
7. Open the downloaded CSV template file in an appropriate application such as **Microsoft Excel**. As shown below, you will see the **Device Name** as the first column followed by columns with names matching the custom properties defined in the gateway template you selected previously. The **Device 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	

4. For each of the gateway devices that you would like to bulk register, enter its **Device-Name** and the required custom properties into the CSV file, one-per-row.



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

5. Ensure to save the file to disk in its original CSV format.
6. 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

-
7. Click **NEXT**.
 8. Under **Register Gateways**, review the details.
 9. Click **Start Registration**.
 10. Click **NEXT**.
 11. Click **DOWNLOAD** to download the CSV file.



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

12. Click **DONE**.

9 Working with INFER™ Agent

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

The INFER™ Agent is a daemon that resides on the Gateway. It acts as a conduit to the INFER™ 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 INFER™.

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*

9.1 Installing INFER™ Agent

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

9.1.1 Installing INFER™ Agent on Linux Gateway

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

1. From the INFER™ Console, click  the top right. The following pop-up appears:



Downloads

Agent Packages (version: 3.0.1-585)

LINUX

WINDOWS

↓ ARM - MLINUX

↓ ARM

↓ AARCH64

↓ X86_64

↓ X86

Campaign CLI (version: 3.0.0)

↓ PACKAGE MANAGEMENT CLI

2. Download the INFER™ Agent tarball **INFER™ Agent (AARCH64)**, or **INFER™ Agent (ARM)** to your local system.
3. Using an FTP/SFTP application such as WinSCP or FileZilla, copy the INFER™ Agent tarball to the gateway file system.
4. Alternatively, you can copy the URL of the Agent from the INFER™ Console. Create a folder for INFER™ using the `mkdir INFER` command and change the permission to `sudo chmod 777 INFER`.
5. On the command-line interface, use CURL or WGET commands to download the Agent. For example:

```
wget -O INFERagent.tar.gz https://iotc001-
INFER.smarthub.ai/api/iotc-agent/<agent-file-name>.tar.gz
```

OR

```
curl -o INFERagent.tar.gz https://iotc001-
INFER.smarthub.ai/api/iotc-agent/<agent-file-name>.tar.gz
```

To specify the output file name:



- WGET uses the upper case 'O',
- CURL uses the lower case 'o'.

6. Extract the Agent tarball on the gateway. For example, `tar -xvzf INFERagent.tar.gz`
7. Change the directory to `iotc-agent` and run `install.sh` as `sudo`.
 - `sudo ./install.sh`
8. Verify whether the Daemon and the Agent services are running. View the **syslog** or use the `journalctl -f` command.



GRPC errors are common and expected at this stage.

You have successfully installed the INFER™ Agent.

9.1.2 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)



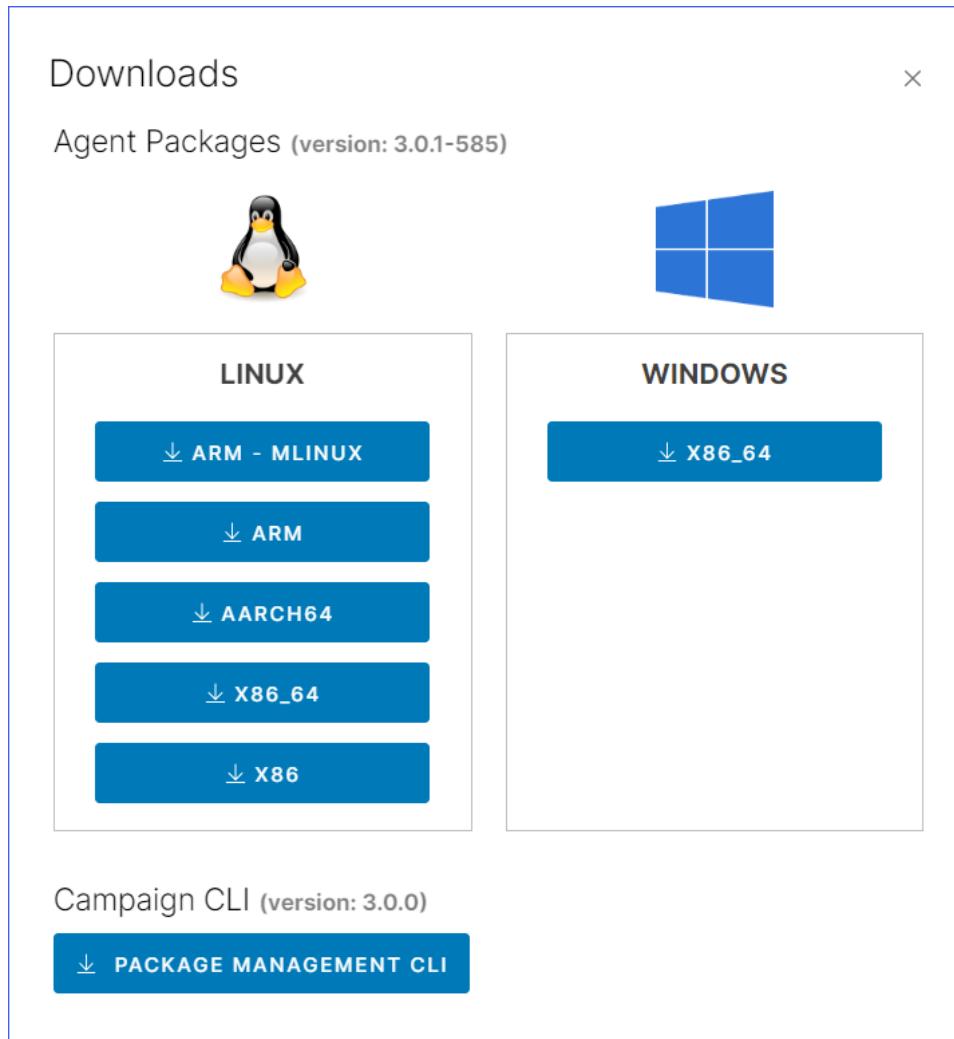
Windows Embedded Standard 7 (x64) requires Windows PowerShell v2.0 or later to be installed on your system.

- Available INFER™ Agent binaries:



- Windows 10 x64 (any edition): *iotc-agent-windows-x86_64-<version>.zip*
- Windows 10 IoT Core ARM: *iotc-agent-windows-arm-<version>.zip*

1. From the INFER™ Console, click 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 zipfile 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 <zip-file> <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. The INFER™ Agent for Windows is installed at *C:\Program Files\SmartHub\iotc-agent*. The following services are also installed:

1. **iotc-agent**

2. **iotc-defclient** (optional)

7. You can also view the event logs using one of the following methods:

1. **Event Viewer** - Create a custom view filter in Event Viewer with the event source as iotc-agentd.
2. **PowerShell Script** - To view the last 10 event logs, run the following PowerShell script:

```
Get-EventLog -LogName Application -Source iotc-agentd -  
Newest 10 | Select-Object -Property TimeGenerated,  
Message | Format-Table -HideTableHeaders -Wrap
```

9.2 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 INFER™ 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.



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

```
error while loading shared libraries: libiotc-agent-sdk.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`

9.2.1 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 IoTCAgent 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=13c425e1-873a-43f0-a529-cb05289a8a40 --type=system" > /tmp/iotc-defclient/input
$ cat /tmp/iotc-defclient/output
```

9.3 Updating INFER™ Agent

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

For information about compatible INFER™ Server and Agent versions, see the *INFER™ Release Notes*.

9.3.1 Update INFER™ Agent Using Campaigns

Update the INFER™ Agent to a newer version using OTA Campaigns.

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

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

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



Ensure that you select the correct version of the IoTCAgent package when upgrading the INFER™ Agent.

For more information about creating and running campaigns, see "Working with Campaigns" on page 141.

9.3.2 Update INFER™ Agent on Multiple Devices

Update the INFER™ Agent on multiple devices from the **Inventory >Devices** tab.

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

Perform the following steps:

1. From the INFER™ Console, go to **Inventory >Devices**.

The **Devices - All Devices** page lists the registered, enrolled, and unenrolled Gateway and Thing devices.

2. Select the devices for which you want to update the agent.



You can also select devices from different templates.

3. From the **... ▾** drop-down, select **Update Agent**.

4. Click **Confirm**.

The **Update Agent Package** confirmation dialog box displays the current version

and the upgrade version of the agent.



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

For more information, see "Tasks" on page 225.

9.3.3 Update INFER™ Agent on a Device from the Console

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

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

Perform the following steps:

1. From the INFER™ Console, go to **Inventory > Devices**.

The **Devices - All Devices** page lists the registered and enrolled gateway and Thing devices.

2. Click the device for which you want to update the agent.
3. From the **Actions** drop-down, 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.

9.3.4 Update 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

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
```



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

10 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" on page 54.
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 devices 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.



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™ user interface and set appropriate **Custom Properties** for the Things.

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

You can either register Things one by one, or in bulk.

10.1 Registering Things One by One

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

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

ZIGILENT_GATE01 ENROLLED Actions ▾

- [Basic Information](#)
- [Properties](#)
- [Metrics](#)
- [Connected devices](#)
- ... ▾

Name
ZIGILENT_GATE01

Device Type
[GATEWAY](#)

Id
0d94b95d-4132-42ed-ad8c-d5a7087183cd

Template Name
Infer-Gateway

Organization
Safe Spaces Inc.

Created (IST)
02/15/2023, 3:06 PM

Modified (IST)
02/15/2023, 3:06 PM



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

ZIGILENT_GATE01 ENROLLED Actions ▾

- [Basic Information](#)
- [Properties](#)
- [Metrics](#)
- [Connected devices](#)
- ... ▾

[ADD DEVICE](#) [BULK REGISTER DEVICES](#)

<input type="checkbox"/>	Name	Device Type	Template Name	Enrollment State	Modified (IST)
					
 					

3. Under **Connected devices**, click **ADD DEVICE**. The **Register Connected Device** pop-up appears as follows:

Register Connected Device

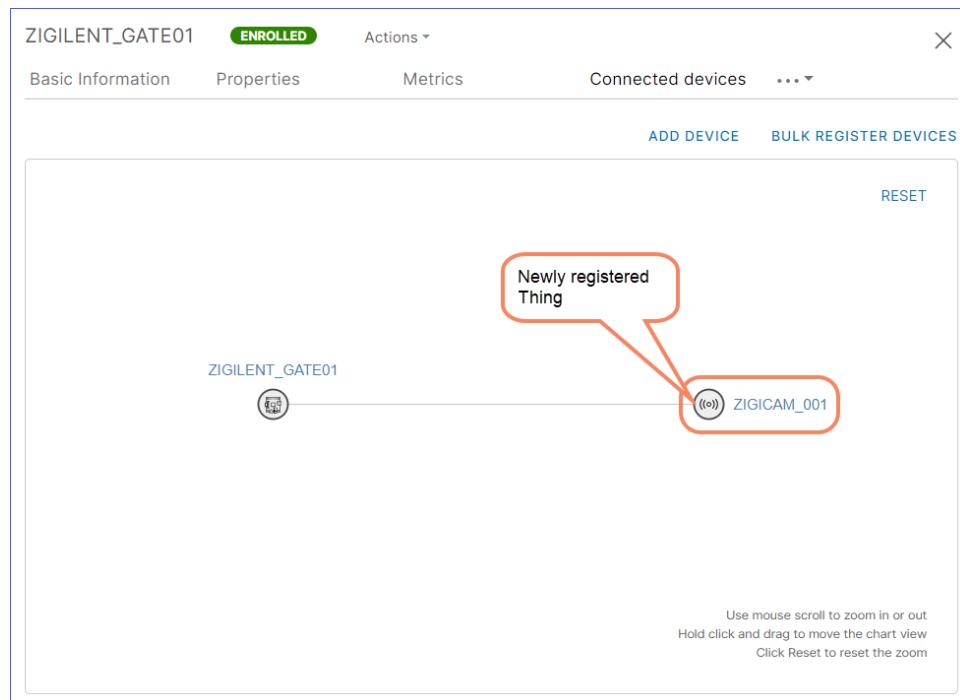
Registering Child for device:
ZIGILENT_GATE01

Device Template
AXIS Camera 3245

Device Name
ZIGICAM_001

CANCEL **REGISTER**

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



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

Inventory - Devices

ZIGICAM_001 REGISTERED Actions ▾

- Basic Information
- Properties
- Metrics
- Connected devices
- ...

Q Search in Properties Search: System Custom

System Properties	EXPAND	
Building: None		
Campus: None		
City: None		
Country: None		
Floor: None		
Password:		
Room: None		
Username: root		
url: 0.0.0.0		

Custom Properties [EXPAND](#)

Custom Properties		
Building: None		
Campus: None		
City: None		
Country: None		
Floor: None		
Password:		
Room: None		
Username: root		
url: 0.0.0.0		

8. 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.



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

10. Click **Save**.

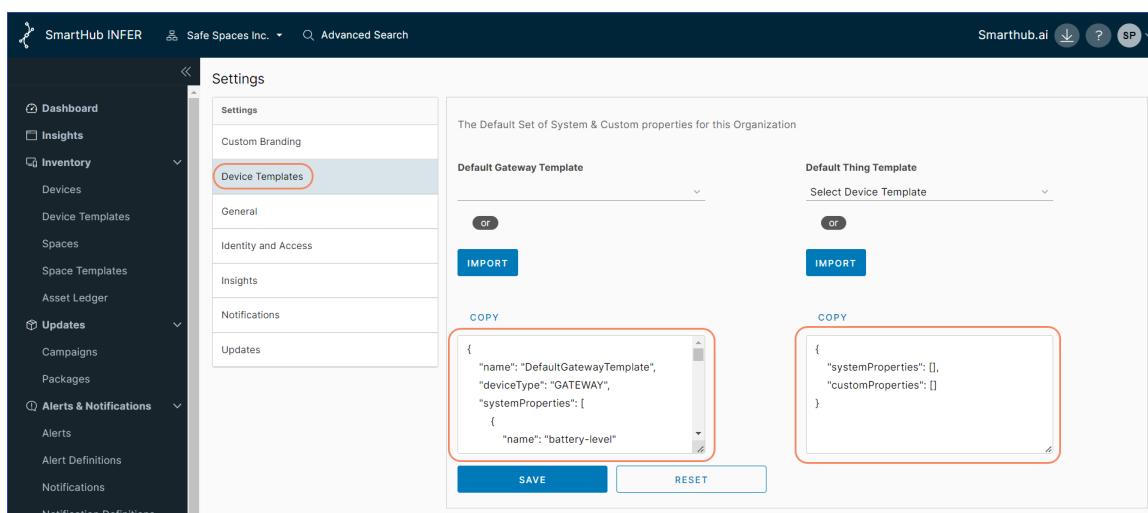
In a few minutes, you can see the Adapter running at the Edge connects with the newly registered Thing based on the Custom properties and **Enroll** the same.

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

10.2 Registering Things in Bulk

To register Things in bulk, perform the following steps:

- 1.** Under **Inventory - Devices**, click the desired gateway.
- 2.** Next, click the **Connected Devices** tab, and click **BULK REGISTER DEVICES**.
The following wizard appears:



```

{
  "name": "DefaultGatewayTemplate",
  "deviceType": "GATEWAY",
  "systemProperties": [
    {
      "name": "battery-level"
    }
  ]
}

{
  "systemProperties": [],
  "customProperties": []
}
  
```

- 3.** Select the desired device template from the drop-down, review the list of custom properties, and click **NEXT**. The following page appears:



	A	B	C	D	E	F	G
1	Device-Name	Adapter-camera-IP	Location-Country	Location-State	Location-City	Location-Floor	Device-Date-Deployment
1	TP-Link Tapo C200	188.37.194.135	India	Karnataka	Bengaluru	GF	01/01/2021
2	Qubo Smart Cam 360	192.168.0.90	United State	Utah	Salt Lake City	Third	
3	TP-Link Tapo C100	192.168.100.1	United State	Arizona	Phoenix		21/08/2021
4	Srihome SH025 camera	192.168.1.108	India		Delhi	FF	

Click button below to upload file
 No file chosen

To create the CSV file, download the CSV template file by [clicking here](#) and fill in the device data as shown in the image above

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

- 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.



The **Device Name** is a mandatory field.

- For each of the devices that you would like to bulk register, enter its Name and the required Custom properties into the CSV file, one-per-row.



You can find the list of Custom properties essential for enrolling the device, in the Adapter documentation or the Thing template's description. For devices 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 Device Details** page and click **Choose File** to upload the CSV file.
- Click **NEXT**. The following **Summary** page appears:

<p>Bulk Register Devices</p> <ul style="list-style-type: none"> 1 Device Template 2 Upload Device Details 3 Summary 	<p>Summary</p> <p>Review details given below and proceed with Bulk Registration</p> <p>Device Template Name AXIS Camera 3245</p> <p>Parent Device Name ZIGILENT_GATE01</p> <p>Number of Devices - 1</p> <p style="text-align: center;">START REGISTRATION</p>	
		BACK CLOSE

9. 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 Devices** tab which now displays all the newly registered Things.
10. Any data errors in the uploaded CSV file will be displayed 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 devices registered.

Resultantly, now, you can see that the status of the onboarded Things've changed from **Registered** to **Enrolled**.

11 Working with Devices

This chapter details the devices' operational states and the various operations you can perform on them from within INFER™:

- Device States
- Sending a Command to INFER™ Agent
- Sending a Command to Multiple Devices
- Bulk device Command Cancellation
- Viewing List of Files
- Viewing List of Devices by State
- Viewing List of Devices by Property
- Updating Bulk Custom Properties on Multiple Devices
- Editing Custom Properties via CSV
- Collecting Metrics using DefaultClient Binary
- Viewing Metric Graphs
- Unenrolling a Device
- Deleting a Device

11.1 Device States

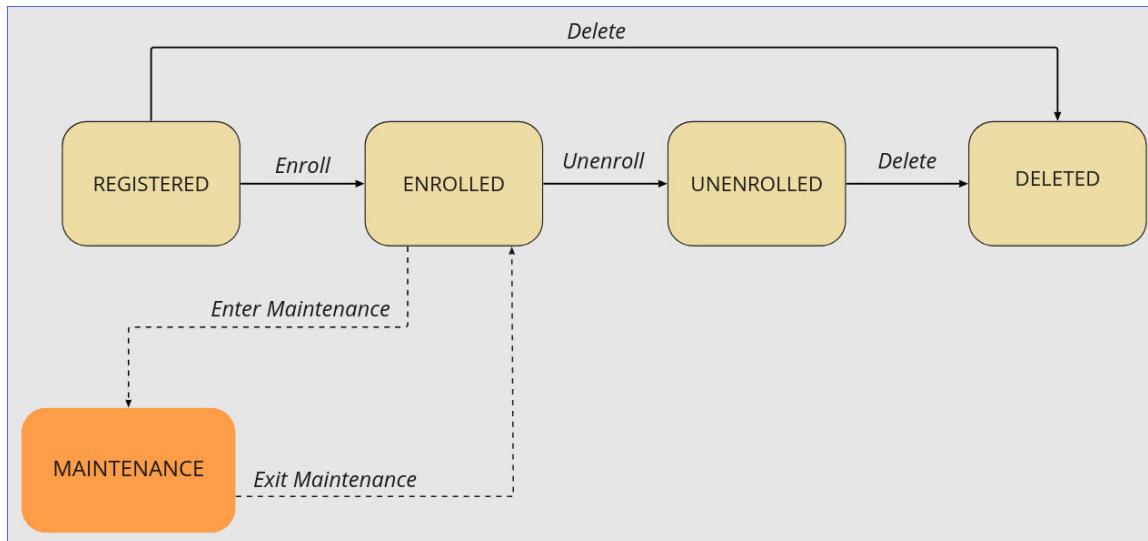
INFER™ displays various operational states that devices can be in during their lifecycle. These states help in understanding and managing the device's behavior and are relevant for device management and monitoring purposes.

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

1. REGISTERED
2. ENROLLED
3. UNENROLLED



4. DELETED, and
5. MAINTENANCE



11.2 Sending a Command to INFER™ Agent

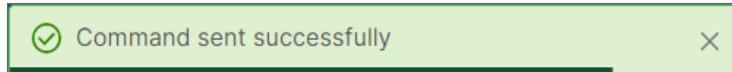
You can send a command to the Agent on your gateway from the INFER™ Console.

1. From the INFER™ Console, go to **Inventory > Devices**.
The **Inventory - Devices** page lists the **Device Type**, **Template Name**, **Enrollment State** and **Connected Devices** of gateways and Thing devices.
2. Click the desired device to which you want to send a command.
3. From the **... ▾** drop-down on the right, select **Commands > SEND COMMAND**.
4. In the **Send Command** pop-up, from the **Select Command** drop-down, select the desired command.
5. Under **Command Type**, enter its arguments.



This command will run with root privilege.

6. Click **SEND COMMAND** to send the command to selected devices, and the following action confirmation message appears:



7. Resultantly, the status of the command is displayed under **Command History**. Click **Refresh** to refresh the status.

11.3 Sending a Command to Multiple Devices

You can select up to 1000 devices of the same template and send a command from the INFER™ Console.



The selected devices must belong to the same template.

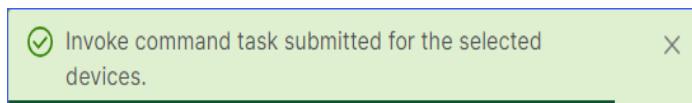
1. From the INFER™ Console, go to **Inventory > Devices**.
2. Select the checkboxes against the devices for which you want to send a command.
3. Go to **Actions** drop-down > **Send Command**. The **Send Command** pop-up appears as follows:

The pop-up window has a blue border and contains the following fields:

- Send Command**
- 2 devices selected**
- Select Command**
Clear Config diff property
- Command Type**
CLIENT_EXECUTE
- Client Identifier**
com.smarthub.camera.adapter.1
- Arguments**
- CANCEL** **SEND COMMAND**



-
4. Under **Select Command**, from the drop-down, select the command.
 5. Click **SEND COMMAND** to send the command to selected devices, and the following action confirmation message appears:



6. Resultantly, the status of the command is displayed under **Command History**.
Click **Refresh** to refresh the status.



You can verify the status of the device command update on multiple devices using the **Tasks** tab.

For more information, see "Tasks" on page 225.

11.4 Bulk Command Cancellation

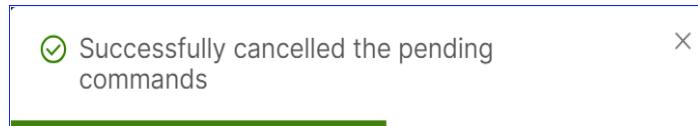
You can cancel device **PENDING** commands in bulk from the INFER™ Console.

Presently, when you perform a command for a device, this new command gets the default state as **PENDING**. Here, the device's agent picks this new command for execution, and once complete it gets 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 device, for example, device unenrollment among others.

1. From the INFER™ Console, go to **Inventory > Devices**.
2. Click the device whose pending commands you desire to cancel.
3. Click **... ▾** drop-down > **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 and the following action confirmation message appears:



11.5 Viewing List of Files

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

Ensure that your device is in **ENROLLED** state.

1. From the INFER™ Console, go to **Inventory > Devices**.
2. Click the device name for which you want to search a file associated with it.
3. From the **... ▾** drop-down, 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 on your local repository.

11.6 Viewing List of Devices by State

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

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

1. From the INFER™ Console, go to **Inventory > Devices**.
2. From the **Enrollment State**: ..., select the state and click **APPLY**.

The list of devices with the selected state is displayed.



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

11.7 Viewing List of Devices by Property

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

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

1. From the INFER™ Console, go to **Inventory > Devices**.
2. From the **Properties** drop-down, select **Search Property Name** and enter the *search value*.
3. Click **OK** and **APPLY**.

The list of devices with the selected property is displayed.



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

11.8 Updating Bulk Custom Properties on Multiple Devices

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

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



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

Perform the following steps:

1. From the INFER™ Console, go to **Inventory > Devices**

The **Inventory - Devices** page lists the registered, enrolled, and unenrolled Gateway and Thing devices.

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



- Devices can be from multiple templates.
- Device state can be Enrolled and Registered.
- Device Type can be GATEWAY and THING.

3. Go to **Actions** drop-down > **Edit Custom Property**. The **Edit Custom Properties** pop-up appears as follows:

Edit Custom Properties

2 devices selected

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

Name	Value
+ Add	

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

Name	Value
+ Add	

Delete
Enter Key(s) to delete from the selected devices

Name	
+ Add	

CANCEL
SAVE

4. Under **Edit**, click **+ Add** and enter keys and value to update custom properties for the selected devices.
5. Under **New**, click **+ Add** and enter keys and value to create custom properties for the selected devices.
6. Under **Delete**, click **+ Add** and enter keys to delete for the selected devices.

-
7. Click **SAVE**. You have successfully updated custom properties in bulk on multiple devices and the following action confirmation message appears:



8. To verify if the values are added, click the device name and **Properties**.
9. Click **Custom Properties**. You can see that the properties are added.
10. To verify if the keys are deleted, click the devices name and **Properties > Custom Properties**.

The keys have been deleted from the **Custom Properties** for the devices.



You can ADD, EDIT, or DELETE any custom property using the bulk command.

11.9 Editing Custom Properties via CSV

You can edit custom properties of devices in bulk using CSV from the INFER™ Console.

1. From the INFER™ Console, go to **Inventory > Devices**.
The **Inventory - Devices** page lists the registered, enrolled, and unenrolled gateway and Thing devices.
2. Click the check boxes against your desired set of devices.
3. Next, at the top right, click **ACTIONS > Edit Custom Properties via CSV**. The following pop-up appears:

Edit Custom Properties via CSV

×

Select all 232 Devices across all pages

Step 1 - Download the CSV contains Custom Properties of the Device(s)

DOWNLOAD CSV

Step 2 - Edit the CSV

In the downloaded CSV,

- Please do not remove/Edit the existing Column headers
 - Please do not edit following Column's cell:
- Device Id
Device Name
Device Type
Device State
Template Name
- New custom property could be added by adding the column header
 - Existing Device'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 CSV format

Step 3 - Upload the Updated CSV file

Drag and drop Or click here to upload the CSV File

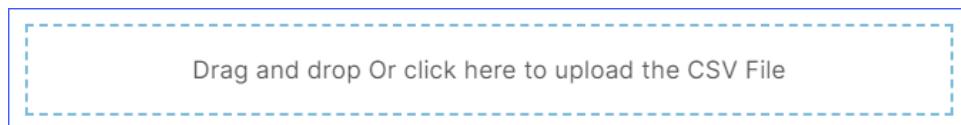
CANCEL

UPDATE

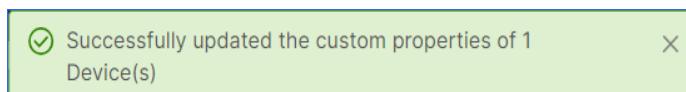
4. Click the check box if you want to select all the listed devices across all pages.
5. Click **DOWNLOAD CSV**.
6. Edit the CSV file by following the rules listed below:
 - a. Do not remove/edit the existing Column headers
 - b. Do not edit following Columns' cells:
 - i. Device Id
 - ii. Device Name
 - iii. Device Type



- iv. Device State
 - v. Template Name
- c. Add new custom property by adding new column header.
 - d. Existing Devices' Custom Properties that match by ID will be updated.
 - e. Rows that do not have the ID will be skipped.
 - f. A custom property will be removed if its value is left empty.
 - g. File format should be saved in CSV format only.
7. Drag and drop the filled CSV file in to the marked area or click the area as shown below:



8. Click **UPDATE**. You have successfully updated the devices' custom properties, and the following action confirmation message appears:



11.10 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 device template. The default metric interval time is 60 seconds.

While creating a device 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.



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 device 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>
```

11.11 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.



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 device, perform the following steps:

1. From the INFER™ Console, go to **Inventory > Devices**.

The Inventory - Devices page lists the registered and enrolled gateway and thing devices.

2. Click the device 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 %)



11.12 Assigning Spaces to Devices

Assigning spaces to devices in INFER™ refers to the physical allocation of locations or areas where the devices are deployed based on the unique requirements and objectives of your edge infrastructure. This process involves carefully deciding where each device should be positioned to optimize their performance, connectivity, and overall effectiveness in your edge network. The goal is to ensure that each device can efficiently communicate with other devices, 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 devices:

- **Coverage and Connectivity:** Ensure that each device has sufficient coverage of the area it needs to monitor or control. The devices 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 devices use radio frequency-based communication (e.g., Wi-Fi, Bluetooth, Zigbee), it's essential to consider potential obstacles that may obstruct the signal. Avoid placing devices in areas with significant physical obstructions that could hinder communication.
- **Power Supply:** As devices require a stable power source, you can ensure that devices located in remote or hard-to-reach locations have easy access to power or use battery-powered devices with suitable battery life.
- **Environmental Conditions:** Consider the environmental conditions (e.g., temperature, humidity, exposure to elements) that each device can withstand. Devices placed in extreme environments may require additional protection or specialized enclosures.
- **Data Collection Requirements:** Understand the specific data collection requirements of each device and position them in locations that offer relevant data insights.
- **Redundancy and Resilience:** Plan for redundancy and resilience by deploying multiple devices in critical areas. Redundancy can help maintain continuous operation even if some devices fail.
- **Security and Privacy:** Be mindful of the security and privacy implications of device placement, especially in sensitive environments. Avoid placing devices 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 devices.
- **Maintenance and Accessibility:** Ensure that devices 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 devices. Minimizing latency can be crucial in certain IoT use cases.

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



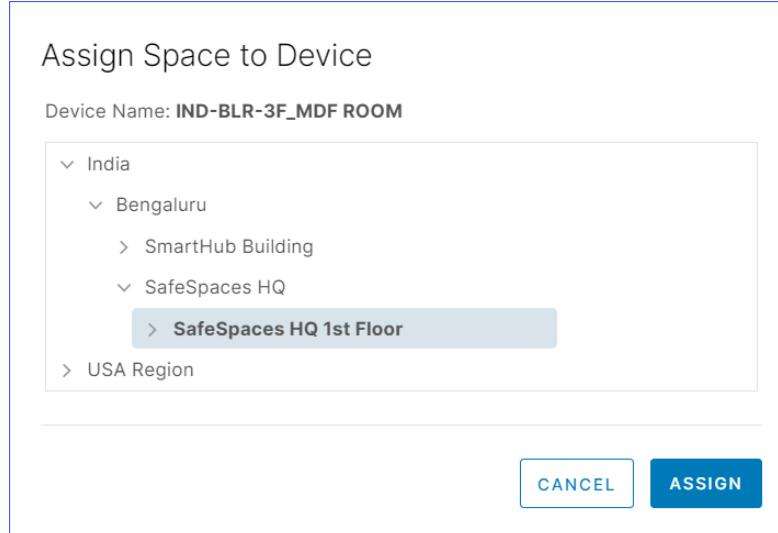
For more information see ""Roles and Permissions" on page 3"

1. From the INFER™ dashboard Console, go to **Devices > Inventory - Devices**.
2. From the listed devices, click the device you desire to assign a space. The device information appears as shown below:

IND-BLR-3F_MDF ROOM
ENROLLED
Actions ▾
X

Name	IND-BLR-3F_MDF ROOM
Device Type	THING
Id	98695d29-f20a-4962-9213-0acf3f8be9e5
Template Name	AXIS Camera 4-digit Series
Parent Device	IND-BLR-SH NUC Gateway 192.168.29.176
Organization	Safe Spaces Inc.
Created (IST)	05/16/2023, 6:05 PM
Modified (IST)	08/02/2023, 12:35 PM
Space	ASSIGN SPACE UNASSIGN SPACE
No Space assigned for this device!	

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



4. Locate and select your desired space under the root location, and click **ASSIGN**. You have successfully assigned a space to a device, and the following action confirmation message appears:



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:



IND-BLR-3F_MDF ROOM ENROLLED Actions ▾

- [Basic Information](#)
- [Properties](#)
- [Metrics](#)
- [Connected Devices](#)
- ... ▾

Name
IND-BLR-3F_MDF ROOM

Device Type
[THING](#)

Id
98695d29-f20a-4962-9213-0acf3f8be9e5

Template Name
AXIS Camera 4-digit Series

Parent Device
IND-BLR-SH NUC Gateway 192.168.29.176

Organization
Safe Spaces Inc.

Created (IST)
05/16/2023, 6:05 PM

Modified (IST)
08/02/2023, 12:35 PM

Space

[ASSIGN SPACE](#) [UNASSIGN SPACE](#)

India > Bengaluru > SafeSpaces HQ > SafeSpaces HQ 1st Floor > IND-BLR-3F_MDF ROOM

11.13 Unassigning Spaces to Devices

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

1. From the INFER™ dashboard Console, go to **Devices > Inventory - Devices**.
2. From the listed devices, click the device you desire to unassign a space. The device information appears as shown below:



IND-BLR-3F_MDF ROOM ENROLLED Actions ▾

Basic Information Properties Metrics Connected Devices ...

Name
IND-BLR-3F_MDF ROOM

Device Type
THING

Id
98695d29-f20a-4962-9213-0acf3f8be9e5

Template Name
AXIS Camera 4-digit Series

Parent Device
IND-BLR-SH NUC Gateway 192.168.29.176

Organization
Safe Spaces Inc.

Created (IST)
05/16/2023, 6:05 PM

Modified (IST)
08/02/2023, 12:35 PM

Space

ASSIGN SPACE UNASSIGN SPACE

No Space assigned for this device!

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

Unassign Space

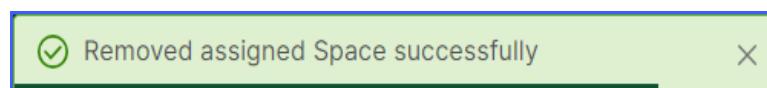
Are you sure you want to Unassign the Space?
This action is permanent and cannot be recovered.

Please type **UNASSIGN** below to confirm action*

Device Name: **IND-BLR-3F_MDF ROOM**

CANCEL UNASSIGN

4. Enter **UNASSIGN** in the text area, and click **UNASSIGN**. You have successfully unassigned a space from a device, and the following action confirmation message appears:



11.14 Unenrolling a Device

To unenroll a gateway and its connected devices that is enrolled to the INFER™ Server, perform the following steps:



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

1. From the INFER™ Console, go to **Inventory > Devices**.

The **Devices - All Devices** page is displayed.

2. Click the gateway or thing device that you want to unenroll.
3. Click the **Actions** drop-down and select **Unenroll**.
4. Confirm your action by clicking **UNENROLL**.

You have successfully unenrolled a device.



This operation also unenrolls the connected devices.

11.15 Deleting Single or Multiple Devices

After unenrolling a device, delete it so that the device no longer appears in the list of devices. You must have the **DELETE_DEVICE** permission to perform this operation.

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

1. From the INFER™ Console, go to **Inventory > Devices**.

The **Inventory - Devices** page is displayed.

2. Select the device 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 device and click **DELETE**.



You have successfully deleted a device.

12 Device Maintenance

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

When a device is put into **MAINTENANCE**, it:

- Caches the device state in the agent,
- Stop alerts generation,
- Stores the reason in the audit log,
- Collects any incoming metrics or any other data.



You can optionally change the state of the devices connected to a device already in **MAINTENANCE**.

This chapter details the various operations you can perform on them in their maintenance state as listed below:

- Entering Maintenance
- Exiting Maintenance

12.1 Entering Maintenance

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



For more information see "Roles and Permissions" on page 3.

1. From the INFER™ Console, go to **Inventory > Devices**.
The **Inventory - Devices** page is displayed.
2. Click the checkbox against the desired device.

3. Go to **Actions > Enter Maintenance**. The **Enter Maintenance** pop-up appears as shown below:

Enter Maintenance

You are about to change the State of the following device(s) to Maintenance.

Please provide a reason for this change*

Degraded performance

Auto-apply this change on children of the selected device(s). [\(i\)](#)

Blr-Office-Awair - ENROLLED

IND-BLR-5F_PF ROOM - ENROLLED

2

[CANCEL](#) [ENTER 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 device(s)**
6. Click **ENTER MAINTENANCE**. You have successfully put the selected things in **Maintenance** state and the following action confirmation message appears:



12.2 Exiting Maintenance

From the MAINTENANCE state, the user can change the device state to ENROLLED. When the user invokes “Exit Maintenance” it changes the device state to ENROLLED, caches the device state in the agent, stores the reason in the audit log as well, and turn on the alerts.

To bring a device 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:



For more information see "Roles and Permissions" on page 3.

1. From the INFER™ Console, go to **Inventory > Devices**.

The **Inventory - Devices** page is displayed.

2. Click the checkbox against the desired device in the list.
3. Go to **Actions > Exit Maintenance**. The **Exit Maintenance** pop-up appears as shown below:

Exit Maintenance

You are about to change the State of the following device(s) to Enrolled.

Please provide a reason for this change*

Moved to new location, back in production

Auto-apply this change on children of the selected device(s). [\(i\)](#)

IND-BLR-5F_IDF ROOM - MAINTENANCE
 IND-BLR-3F_MDF ROOM - MAINTENANCE

2

[CANCEL](#) [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 device(s)**
6. Click **EXIT MAINTENANCE**. You have successfully reverted the selected things' state into **ENROLLED** state and the following action confirmation message appears:



✓ 0 Gateway(s) and 2 Thing(s) exited maintenance state
successfully

X

13 Device 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 device to another gateway with better coverage.
- **Load Balancing:** In situations where multiple gateways are deployed, devices 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:** If 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

the connected devices are moved to an alternative gateway for uninterrupted connectivity and functionality.

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



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**.

13.1 Migration Checklist

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 "Device Migration" on the previous page
2. **Agent Version:** Verify whether both the old parent gateway and the new parent gateway have agents with versions equal to or greater than **v3.0.1-593**. For more information on updating INFER™ Agent, see "Updating INFER™ Agent" on page 90.
3. **Organization Alignment:** Verify whether the devices and their connected devices belong to the same organization.
4. **Single Gateway:** Verify whether the devices and their connected devices belong to a single root gateway.
5. **Gateway Hierarchy:** Only devices 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 device's device 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.



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 devices and their connected things.

13.2 Migrating Things & Gateways

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

- Under **Inventory - Devices**, select the check boxes of things that need to be migrated.



- Make sure that the **Enrollment State** of the things' you have selected for migration are in **MAINTENANCE** state. For more information on putting devices into **MAINTENANCE** state, see "Device Migration" on page 123.
- Currently INFER™ supports only migration of devices that are things (not gateways).
- Selected devices needs to have same parent gateway for migration.

- Go to **Actions > Device Migration**. The **Device Migration** pop-up appears as shown below:

Device Migration																										
1 Select Devices 2 Parent Device 3 Review	Select Devices Only device(s) that are thing and in maintenance state can be migrated to another device. Selected devices needs to have same parent gateway for migration. <small>Click on the  icon to put the device into the maintenance state for migration. Only thing(s) in maintenance state are selectable.</small> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;"><input checked="" type="checkbox"/></th> <th>Name</th> <th>Device Type</th> <th>Enrollment State</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td>IND-BLR-SF_IDF ROOM</td> <td>THING</td> <td>MAINTENANCE</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>IND-BLR-3F_MDF ROOM</td> <td>THING</td> <td>MAINTENANCE</td> </tr> <tr> <td><input type="checkbox"/></td> <td>IND-BLR-SH NUC Gateway 192.168.29.176</td> <td>GATEWAY</td> <td>ENROLLED</td> </tr> <tr> <td><input type="checkbox"/></td> <td>IND-BLR-3F_ENTRY ROOM</td> <td>THING</td> <td>ENROLLED </td> </tr> <tr> <td colspan="4" style="text-align: center;">2</td> </tr> </tbody> </table> <div style="text-align: right; margin-top: 10px;"> CANCEL NEXT </div>		<input checked="" type="checkbox"/>	Name	Device Type	Enrollment State	<input checked="" type="checkbox"/>	IND-BLR-SF_IDF ROOM	THING	MAINTENANCE	<input checked="" type="checkbox"/>	IND-BLR-3F_MDF ROOM	THING	MAINTENANCE	<input type="checkbox"/>	IND-BLR-SH NUC Gateway 192.168.29.176	GATEWAY	ENROLLED	<input type="checkbox"/>	IND-BLR-3F_ENTRY ROOM	THING	ENROLLED 	2			
<input checked="" type="checkbox"/>	Name	Device Type	Enrollment State																							
<input checked="" type="checkbox"/>	IND-BLR-SF_IDF ROOM	THING	MAINTENANCE																							
<input checked="" type="checkbox"/>	IND-BLR-3F_MDF ROOM	THING	MAINTENANCE																							
<input type="checkbox"/>	IND-BLR-SH NUC Gateway 192.168.29.176	GATEWAY	ENROLLED																							
<input type="checkbox"/>	IND-BLR-3F_ENTRY ROOM	THING	ENROLLED 																							
2																										

- In the previous step, in case you selected a device which was not in the **MAINTENANCE** state, click  as highlighted above to put the device into the

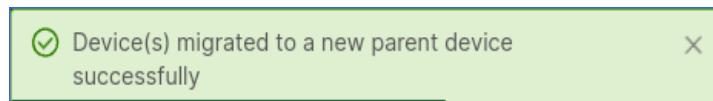


maintenance state.

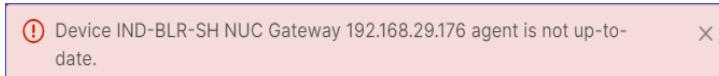


Only things (not gateways) in maintenance state are selectable.

4. Click **NEXT**.
5. Under **Parent Device**, select the desired new parent device from the drop-down, and click **NEXT**.
6. Under **Review**, review the information and click **SAVE**. You have successfully migrated the selected devices to a new parent device, and the following action confirmation message appears:



7. However, if the agent running in the parent device is not up-to-date, the migration has failed and the following error message appears:



14 Working with Asset Ledger

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

14.1 Creating an Asset Folder

To create a new asset folder in INFER™, you must have the VIEW_ASSET_LEDGER and EDIT_ASSET_LEDGER permissions associated with the Organization Administrator Group, and perform the following steps:



For more information see "Roles and Permissions" on page 3.

1. From the INFER™ Console, go to **Inventory > Asset Ledger**. The **Asset Folders** page is displayed as shown below:

Name	Records	Created (IST)	Actions
Plant 1 Inventory	1960	10/26/2022, 12:29 PM	... ▾
Plant 2 Inventory	121	10/26/2022, 12:32 PM	... ▾
Licenses	114	10/26/2022, 12:33 PM	... ▾
Controllers	251	10/26/2022, 12:33 PM	... ▾

2. Click **Create Folder > Using CSV File** as highlighted above. The **New Folder | CSV** wizard appears.
3. Under **Name**, enter the desired asset folder name.
4. Under **Upload the CSV File**, drag/drop the CSV file you are creating. This CSV must carry relevant asset columns as highlighted in example shown below:

A	B	C	D	E	
1	Location	Device Name	IP Address	Device Category	Model
2	NASHVILLE	1FL BMS ROOM	169.254.208.50	Cameras	X0542-MK
3	NASHVILLE	1FL SOC DOOR	169.254.208.51	Cameras	X0543-LVII
4	NASHVILLE	2FL IDF ROOM	169.254.208.52	Cameras	X0544-LVI
5	COLUMBIA DTC	2FL NORTH LIFT LOBBY	169.254.207.78	Cameras	X0545-LVI
6	COLUMBIA DTC	2FL SOUTH LIFT LOBBY	169.254.207.79	Cameras	X0546-LVI
7	COLUMBIA DTC	2FL STAIRCASE 1	169.254.207.80	Cameras	X0547-LVI
8	COLUMBIA DTC	2FL STAIRCASE 2	169.254.207.81	Cameras	X0548-LVI
9	COLUMBIA DTC	2FL STAIRCASE 3	169.254.207.82	Cameras	X0549-MK
10	COLUMBIA DTC	3FL IDF ROOM	169.254.207.83	Cameras	X0550-MK
11	COLUMBIA DTC	3FL IT SOC ROOM	169.254.207.84	Cameras	X0551-MK
12	COLUMBIA DTC	3FL NORTH LIFT LOBBY	169.254.207.85	Cameras	X0552-MK
13	COLUMBIA DTC	3FL SOUTH LIFT LOBBY	169.254.207.86	Cameras	X0553-MK
14	COLUMBIA DTC	3FL STAIRCASE 1	169.254.207.87	Cameras	X0554-LNL
15	COLUMBIA DTC	3FL STAIRCASE 2	169.254.207.88	Cameras	X0555-LNL
16	NEW YORK	3FL STAIRCASE 3	169.254.209.52	Cameras	X0556-LNL
17	LOS ANGELES	3FL VC3	169.254.205.10	Cameras	X0557-LNL
18	LOS ANGELES	4FL IDF ROOM	169.254.205.11	Cameras	X0558-LNL
19	LOS ANGELES	4FL NORTH LIFT LOBBY	169.254.205.12	Cameras	X0559-LVI
20	LOS ANGELES	4FL SOUTH LIFT LOBBY	169.254.205.13	Cameras	X0560-LVI
21	LOS ANGELES	4FL STAIRCASE 1	169.254.205.14	Cameras	X0561-LVI
22	LOS ANGELES	4FL STAIRCASE 2	169.254.205.15	Cameras	X0562-LVI
23	SEATTLE	4FL STAIRCASE 3	169.254.277.88	Cameras	X0563-LVI
24	MTV	GF GAS BANK ROOM	169.254.268.27	Cameras	X0564-LVI
25	MTV	5FL NORTH LIFT LOBBY	169.254.268.28	Cameras	X0565-LVI
26	DENVER DTC	5FL STAIRCASE 3	169.254.289.94	Cameras	X0566-LVI

5. On upload, to confirm your file upload, you can see the preview of the 1st row data as **Sample Row** as shown below:

New Folder | CSV

Name
Cameras

Upload the CSV File

Camera Inventory.csv

Preview of an Uploaded Sample Row

```
{
  "location": "NASHVILLE",
  "device-name": "1FL BMS ROOM",
  "ip-address": "169.254.208.50",
  "device-category": "Cameras",
  "model": "X0542-MK"
}
```

CANCEL NEXT

6. Click **NEXT**. The following modal view appears as shown below:

New Folder | CSV

Choosing the option to edit allows you to evaluate the auto-assigned values for each field's component, input type, & other detail.

Basic Details			
	Field	Filter	Sortable
<input type="checkbox"/>	Location	--	--
<input type="checkbox"/>	Device Name	--	--
<input type="checkbox"/>	Ip Address	--	--
<input type="checkbox"/>	Device Category	--	--
<input type="checkbox"/>	Model	--	--

✓ Applied -- n/a << < 1 / 1 > >>

CANCEL BACK SAVE

14.2 Modifying the Default Field Group

- Under **Field Groups**, the previously uploaded CSV file's auto-assigned values show up under the **Basic Details** default field group.

Click  as highlighted above to modify each field's component, input type, and other details as shown below:

Field label

Field name ⓘ

Component

Textbox

Input type

Text

Filter **Sort**

Done **Cancel**

2. Enter the **Field label** and **Field name** details.
3. Select the **Component** and **Input type** values from their drop-downs.
4. Click the **Filter** and **Sort** toggle switches to enable filtering and sorting of this field's values.
5. Click **DONE** to return to the field group.
6. Click **+ Field** to add new fields to a group and enter this field's component, input type, and other details as explained above.
7. To delete a field, select its checkbox and click .

14.3 Creating a New Field Group

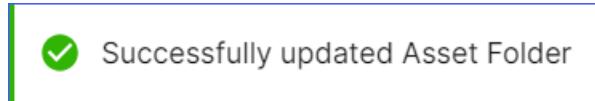
1. Next, when the uploaded CSV file's field values exceed 10 fields, for better usability, you can create logical field groups. Click **+ Field Group** to create a new field group.

2. Under **Group label**, enter the new group's label and click **DONE**.

3. Click  to add new fields to the empty group.

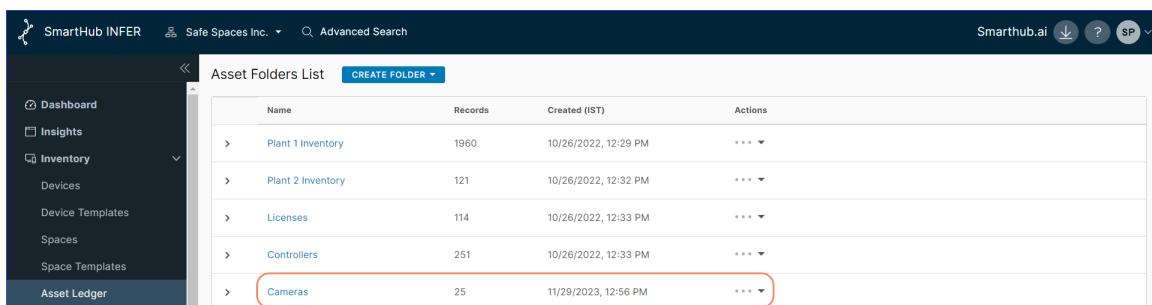
14.4 Moving Fields between Groups

1. To move a field, select its checkbox and click .
2. Next, under **Target Field Group**, select the desired group from the drop-down and click **MOVE**. The moved field appears in the target group.
3. Click **SAVE**. You have successfully updated an asset folder, and the following action confirmation message appears:



 Successfully updated Asset Folder

You can see the newly created asset folder as shown below:



The screenshot shows the SmartHub INFER interface with the 'Asset Ledger' menu item selected in the sidebar. The main area displays a table titled 'Asset Folders List' with the following data:

Name	Records	Created (IST)	Actions
Plant 1 Inventory	1960	10/26/2022, 12:29 PM	...
Plant 2 Inventory	121	10/26/2022, 12:32 PM	...
Licenses	114	10/26/2022, 12:33 PM	...
Controllers	251	10/26/2022, 12:33 PM	...
Cameras	25	11/29/2023, 12:56 PM	...

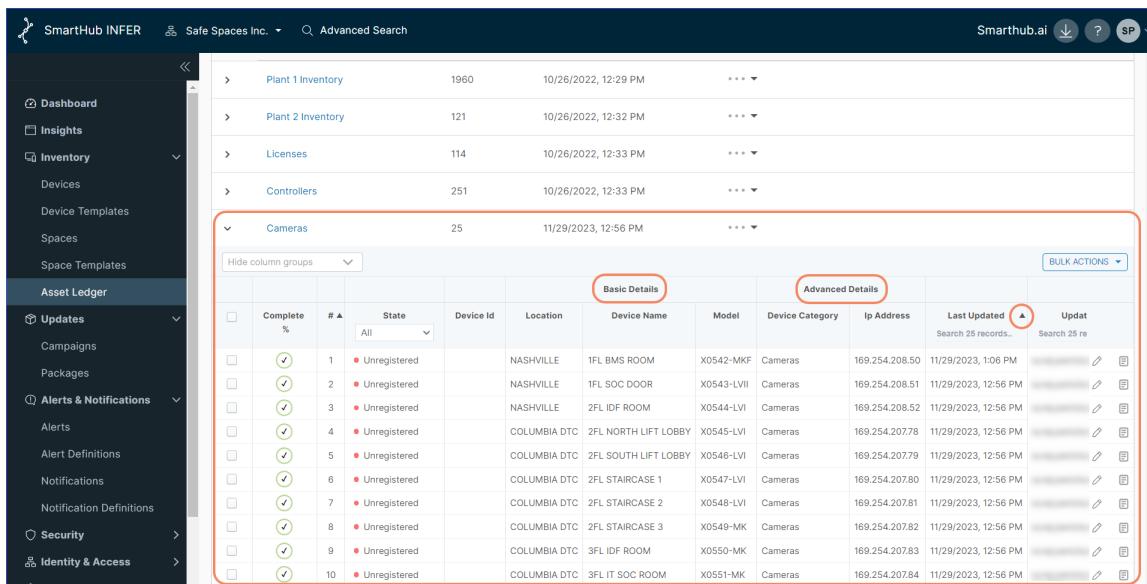
14.5 Working with Asset Tables

For a tabulated view of your asset folders, perform the following steps:

1. Click the drop-down of any folder as highlighted below:



The following view appears:



		Basic Details		Advanced Details							
<input type="checkbox"/>	Complete %	# ▲	State	Device Id	Location	Device Name	Model	Device Category	Ip Address	Last Updated	Updated By
<input type="checkbox"/>	✓	1	● Unregistered		NASHVILLE	1FL BMS ROOM	X0542-MKF	Cameras	169.254.208.50	11/29/2023, 1:06 PM	
<input type="checkbox"/>	✓	2	● Unregistered		NASHVILLE	1FL SOC DOOR	X0543-LVII	Cameras	169.254.208.51	11/29/2023, 12:56 PM	
<input type="checkbox"/>	✓	3	● Unregistered		NASHVILLE	2FL IDF ROOM	X0544-LVI	Cameras	169.254.208.52	11/29/2023, 12:56 PM	
<input type="checkbox"/>	✓	4	● Unregistered		COLUMBIA DTC	2FL NORTH LIFT LOBBY	X0545-LVI	Cameras	169.254.207.78	11/29/2023, 12:56 PM	
<input type="checkbox"/>	✓	5	● Unregistered		COLUMBIA DTC	2FL SOUTH LIFT LOBBY	X0546-LVI	Cameras	169.254.207.79	11/29/2023, 12:56 PM	
<input type="checkbox"/>	✓	6	● Unregistered		COLUMBIA DTC	2FL STAIRCASE 1	X0547-LVI	Cameras	169.254.207.80	11/29/2023, 12:56 PM	
<input type="checkbox"/>	✓	7	● Unregistered		COLUMBIA DTC	2FL STAIRCASE 2	X0548-LVI	Cameras	169.254.207.81	11/29/2023, 12:56 PM	
<input type="checkbox"/>	✓	8	● Unregistered		COLUMBIA DTC	2FL STAIRCASE 3	X0549-MK	Cameras	169.254.207.82	11/29/2023, 12:56 PM	
<input type="checkbox"/>	✓	9	● Unregistered		COLUMBIA DTC	3FL IDF ROOM	X0550-MK	Cameras	169.254.207.83	11/29/2023, 12:56 PM	
<input type="checkbox"/>	✓	10	● Unregistered		COLUMBIA DTC	3FL IT SOC ROOM	X0551-MK	Cameras	169.254.207.84	11/29/2023, 12:56 PM	

2. You can notice the field groups as highlighted above. You can also see that **Complete**, **State**, **Device Id**, **Last Updated**, and **Updated By** columns/fields appear newly added by INFER™ along with the data you uploaded in the previously.



- Under **Complete**, the percentage shows the extent of completeness of that asset's uploaded data fields in any field group. This helps you to detect empty asset fields across the asset folder and update the same using .
- Under **State**, all newly uploaded assets appear and begin as **Unregistered**. Upon registration, they will appear as **Registered** along with their device id appearing under **Device Id** column.

14.5.1 Bulk Actions

When you need to save your time while editing, registering and deleting assets, you can

select the desired checkboxes and click **BULK ACTIONS** to perform the following actions:

- **Edit Assets via CSV**
- **Edit Assets via Column**
- **Register Assets**
- **Delete Assets**

as highlighted below:

					Basic Details		Advanced Details				BULK ACTIONS
<input type="checkbox"/>	Complete %	# ▲	State	Device Id	Location	Device Name	Model	Device Category	Ip Address	Last Update	<input type="button" value="Edit Assets via CSV"/> <input type="button" value="Edit Assets via Column"/> <input type="button" value="Register Assets"/> <input type="button" value="Delete Assets"/>
<input type="checkbox"/>		1	● Unregistered		NASHVILLE	1FL BMS ROOM	X0542-MKFG	Cameras	169.254.208.50	12/05/2023, 11:29:20 AM	
<input checked="" type="checkbox"/>		2	● Unregistered		NASHVILLE	1FL SOC DOOR	X0543-LVII	Cameras	169.254.208.51	11/29/2023, 12:56 PM	suraj.panici
<input type="checkbox"/>		3	● Unregistered		NASHVILLE	2FL IDF ROOM	X0544-LVI	Cameras	169.254.208.52	11/29/2023, 12:56 PM	suraj.panici
<input checked="" type="checkbox"/>		4	● Unregistered		COLUMBIA DTC	2FL NORTH LIFT LOBBY	X0545-LVI	Cameras	169.254.207.78	11/29/2023, 12:56 PM	suraj.panici
<input checked="" type="checkbox"/>		5	● Unregistered		COLUMBIA DTC	2FL SOUTH LIFT LOBBY	X0546-LVI	Cameras	169.254.207.79	11/29/2023, 12:56 PM	suraj.panici
<input type="checkbox"/>		6	● Unregistered		COLUMBIA DTC	2FL STAIRCASE 1	X0547-LVI	Cameras	169.254.207.80	11/29/2023, 12:56 PM	suraj.panici
<input checked="" type="checkbox"/>		7	● Unregistered		COLUMBIA DTC	2FL STAIRCASE 2	X0548-LVI	Cameras	169.254.207.81	11/29/2023, 12:56 PM	suraj.panici
<input checked="" type="checkbox"/>		8	● Unregistered		COLUMBIA DTC	2FL STAIRCASE 3	X0549-MK	Cameras	169.254.207.82	11/29/2023, 12:56 PM	suraj.panici
<input checked="" type="checkbox"/>		9	● Unregistered		COLUMBIA DTC	3FL IDF ROOM	X0550-MK	Cameras	169.254.207.83	11/29/2023, 12:56 PM	suraj.panici
<input type="checkbox"/>		10	● Unregistered		COLUMBIA DTC	3FL IT SOC ROOM	X0551-MK	Cameras	169.254.207.84	11/29/2023, 12:56 PM	suraj.panici

14.5.2 Editing Assets via CSV

To edit assets in a folder using a CSV file, perform the following actions:

1. Click the desired asset checkboxes.
2. From the **BULK ACTIONS** drop-down, select **Edit Assets via CSV**. The **Edit Assets via CSV** pop-up appears.
3. Click **EXPORT ASSET RECORDS** to download your asset records in a CSV file.
4. Open the downloaded CSV file, and make the desired changes, save the changes.
5. Upload the modified CSV file.

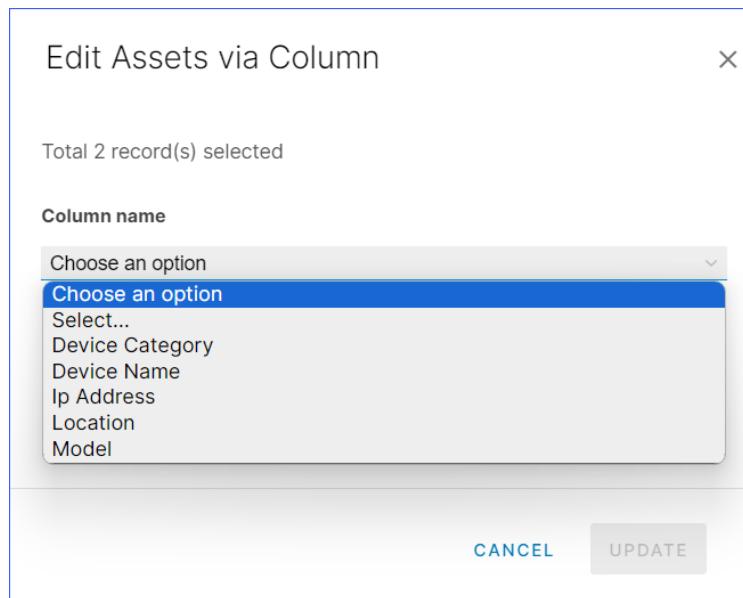


Existing asset records that match by ID will be updated. Records that do not exist will be skipped and Without ID column in the file will be added as new entries.

14.5.3 Editing Assets via Column

To edit assets in a folder using columns, perform the following actions:

1. Click the desired asset checkboxes.
2. From the **BULK ACTIONS** drop-down, select **Edit Assets via Column**. The **Edit Assets via Column** pop-up appears as shown below:



3. Choose the desired asset parameter from the drop-down, enter the new parameter.
4. Click **UPDATE**. You have successfully updated an asset folder, and the following action confirmation message appears:

 Successfully updated 2 Asset record(s)

14.5.4 Registering Assets

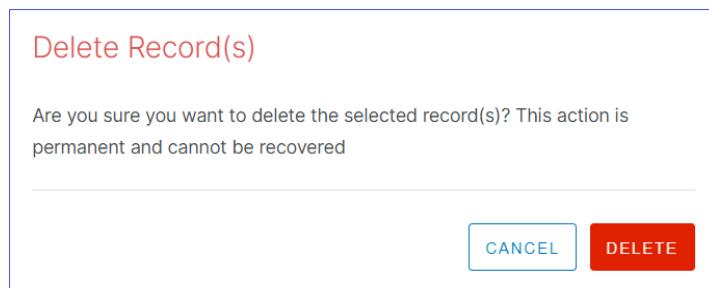
To register assets in a folder into INFER™, perform the following actions:

1. Click the desired asset checkboxes.
2. From the **BULK ACTIONS** drop-down, select **Register Assets**. The **Register Assets** pop-up appears.
3. Next, under **Device name column**, select the device name column from the drop-down.
4. Under **Gateway**, select the desired gateway from the drop-down.
5. Under **Device template**, select the desired device template from the drop-down.
6. Under **Custom Properties**, click the desired custom property checkboxes.
7. Click **REGISTER**.

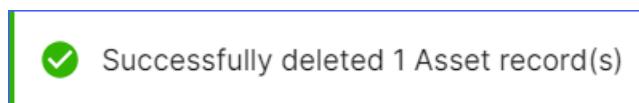
14.5.5 Deleting Records

To delete assets in a folder using columns, perform the following actions:

1. Click the desired asset checkboxes.
2. From the **BULK ACTIONS** drop-down, select **Delete Records**. The **Delete Record(s)** pop-up appears as shown below:



3. Click **DELETE** to delete the selected records. You have successfully deleted asset records, and the following action confirmation message appears:



14.5.6 Hiding Field Groups

When you need to focus and work on an individual field group within an asset folder, perform the following steps:

1. Click **Hide Field Groups** drop-down as highlighted below:



The screenshot shows a table with columns for Device ID, Location, Device Name, Model, Device Category, Ip Address, Last Updated, and Updated. The first two columns have dropdown menus labeled 'Basic Details' and 'Advanced Details'. The 'Basic Details' checkbox is checked, and the 'Advanced Details' checkbox is unchecked. The table contains three rows of asset data.

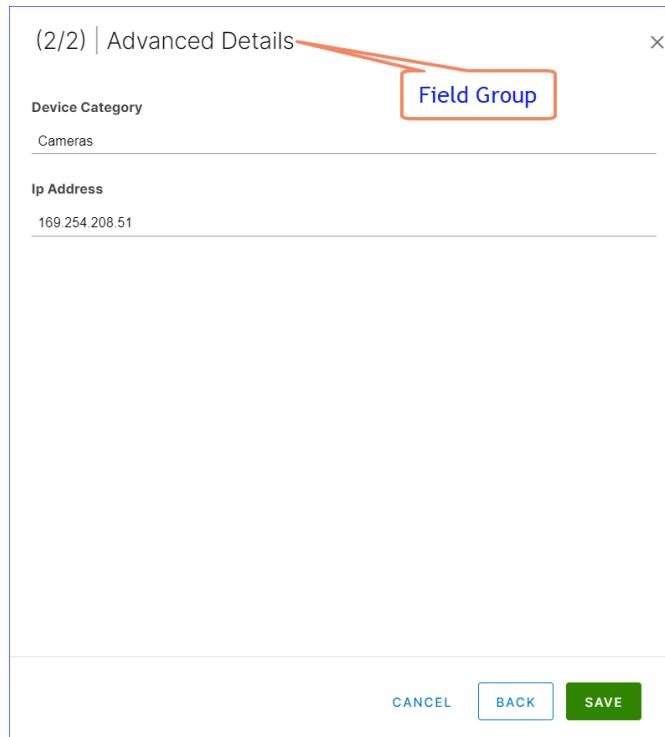
Basic Details		Advanced Details				
Device ID	Location	Device Name	Model	Device Category	Ip Address	Last Updated
X0542-MKFG	NASHVILLE	1FL BMS ROOM	X0542-MKFG	Cameras	169.254.208.50	12/05/2023, 11:38 AM
X0543-LVII	NASHVILLE	1FL SOC DOOR	X0543-LVII	Cameras	169.254.208.51	11/29/2023, 12:56 PM
X0544-LVI	NASHVILLE	2FL IDF ROOM	X0544-LVI	Cameras	169.254.208.52	11/29/2023, 12:56 PM

2. Click the required checkboxes to hide field groups from view.

14.5.7 Updating Individual Assets

To modify individual asset values, perform the following actions:

1. Click  of any asset. The following wizard appears:



(2/2) | Advanced Details

Device Category

Cameras

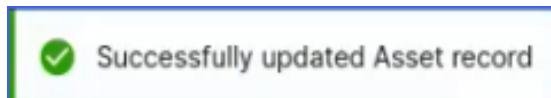
Ip Address

169.254.208.51

Field Group

CANCEL BACK **SAVE**

2. Make required changes to various asset filed values and click **SAVE**. You have successfully updating an asset record, and the following action confirmation message appears:



14.5.8 Records Change Log

To view the asset records change log, perform the following actions:

1. Click  to open the following pop-up.

Records Change Log

Date Range Filter: dd-yyyy-- -- dd-yyyy -- -- Apply

Updated At	Updated By
01/01/ 5:30 AM	
01/01/ 5:30 AM	
1 { 2 - "model": "X0542-MK" 3 "location": "NASHVILLE", 4 "ip-address": "169.254.208.50", 5 "device-name": "1FL BMS ROOM", 6 - "device-category": "Cameras" 7 }	1 { 2 + "model": "X0542-MKF" 3 "location": "NASHVILLE", 4 + "device_id": "", 5 "ip-address": "169.254.208.50", 6 "device-name": "1FL BMS ROOM", 7 + "device-category": "Cameras", 8 + "enrollment_state": "" 9 }

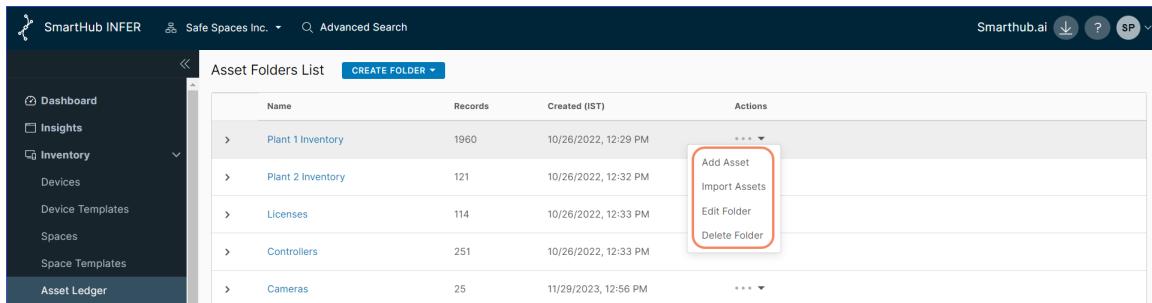
DONE

2. Specify your desired date range in the **Date Range Filter**'s calendar widget and click **Apply**.
3. Click the highlighted drop-down to view the changed details highlighted in Green.
4. Click **DONE** to close the pop-up.

14.6 Adding Assets

Besides uploading asset data into INFER™ via [CSV](#) file, you can also add individual assets by performing the following actions:

1. Under the **Actions** column, click **•••** against any asset folder and select **Add Asset** from the drop-down as shown below:



Name	Records	Created (IST)	Actions
Plant 1 Inventory	1960	10/26/2022, 12:29 PM	•••
Plant 2 Inventory	121	10/26/2022, 12:32 PM	•••
Licenses	114	10/26/2022, 12:33 PM	•••
Controllers	251	10/26/2022, 12:33 PM	•••
Cameras	25	11/29/2023, 12:56 PM	•••

2. Enter the values for field groups, and click **SAVE**. You have successfully added an asset record, and the following action confirmation message appears:

 Successfully added Asset record

14.7 Importing Assets

If you have a large number of assets, you can upload them into the Asset Ledger using a CSV file. To import assets, perform the following actions:

1. Under the **Actions** column, click **•••** against any asset folder and select **Import Assets** from the drop-down. The **Import Assets** pop-up appears.
2. Click **DOWNLOAD CSV TEMPLATE** to download the CSV import template file, which carry the following basic columns:
 - a. Device Category
 - b. Device Name
 - c. Ip Address
 - d. Location
 - e. Model
3. Open the downloaded CSV file, fill in the above fields, add more fields as desired, and save the changes.
4. Drag/drop or browse to upload the CSV file, and click **IMPORT**. You have successfully added asset records to the folder, and the following action confirmation message appears:

 Successfully added 1 records to Asset Folder

14.8 Editing Asset Folders

You can change an existing asset folder information by performing the following actions:



1. Under the **Actions** column, click **...** against any asset folder, select **Update Folder** from the drop-down. The **Update Folder** pop-up appears.
2. Make desired updates to the **Field Groups** and **Field** values and click **UPDATE**. You have successfully updated the asset folder, and the following action confirmation message appears:

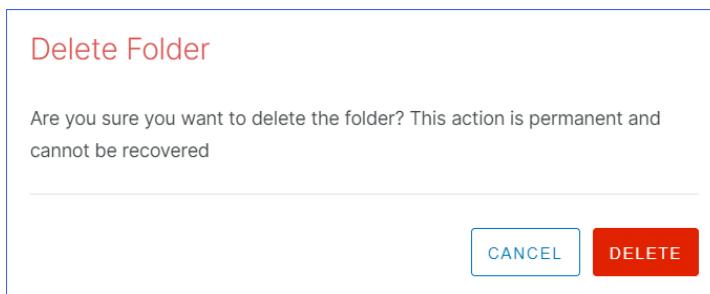


Successfully updated Asset Folder

14.9 Deleting Asset Folders

You can delete an asset folder only when it is empty. Delete an asset folder by performing the following actions:

1. Click all the asset checkboxes.
2. From the **BULK ACTIONS** drop-down, select **Delete Records**.
3. Next, under the **Actions** column, click **...** against any asset folder and select **Delete Folder** from the drop-down. The **Delete Folder** pop-up appears as shown below:



Are you sure you want to delete the folder? This action is permanent and cannot be recovered.

4. Click **DELETE** to delete the selected folder. You have successfully deleted asset folder, and the following action confirmation message appears:



Successfully deleted Asset Folder

15 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 INFER™'s **Campaigns** sub-module.

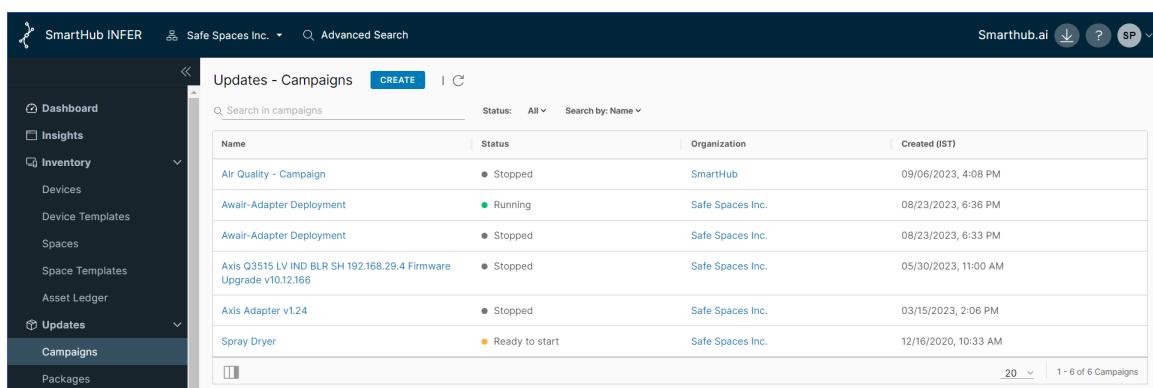
15.1 What is a Campaign?

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 INFER™ 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,
- end a campaign,
- add a distribution select query to the campaign, and
- associate update packages to the devices in your campaign.



Name	Status	Organization	Created (IST)
Air Quality - Campaign	● Stopped	SmartHub	09/06/2023, 4:08 PM
Awair-Adapter Deployment	● Running	Safe Spaces Inc.	08/23/2023, 6:36 PM
Awair-Adapter Deployment	● Stopped	Safe Spaces Inc.	08/23/2023, 6:33 PM
Axis Q3515 LV IND BLR SH 192.168.29.4 Firmware Upgrade v10.12.166	● Stopped	Safe Spaces Inc.	05/30/2023, 11:00 AM
Axis Adapter v1.24	● Stopped	Safe Spaces Inc.	03/15/2023, 2:06 PM
Spray Dryer	● Ready to start	Safe Spaces Inc.	12/16/2020, 10:33 AM

15.1.1 Distribution Select Query

Using the **Campaigns** sub-module, you can specify an existing Distribution Select Query or create a new query to run a campaign. The Distribution Select Query periodically matches a subset of all the registered devices that fulfill the query.

To add specific devices to the campaign, call the **addTargetGateways** API. For more information about Campaign Management APIs, see the *SmartHub INFER API Reference Guide*.

15.2 Campaign Approvals

If your campaigns (OTA) require an approval before starting, toggle the **Enable Approval** option under the **Settings > Updates** tab. For information about enabling campaign approvals, see "Settings" on page 211. Users with permissions to edit organization settings can set the approvals for campaigns. Users with campaign approval permissions can approve a campaign.



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

By default, campaigns do not require an approval when you create it unless you configure your organization's settings to check for campaign approvals. By default, 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.

15.2.1 Campaign Approval Use Cases

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



For more information see "Roles and Permissions" on page 3.

-
- CREATE_PACKAGE
 - EDIT_PACKAGE
 - DELETE_PACKAGE
 - VIEW_PACKAGE

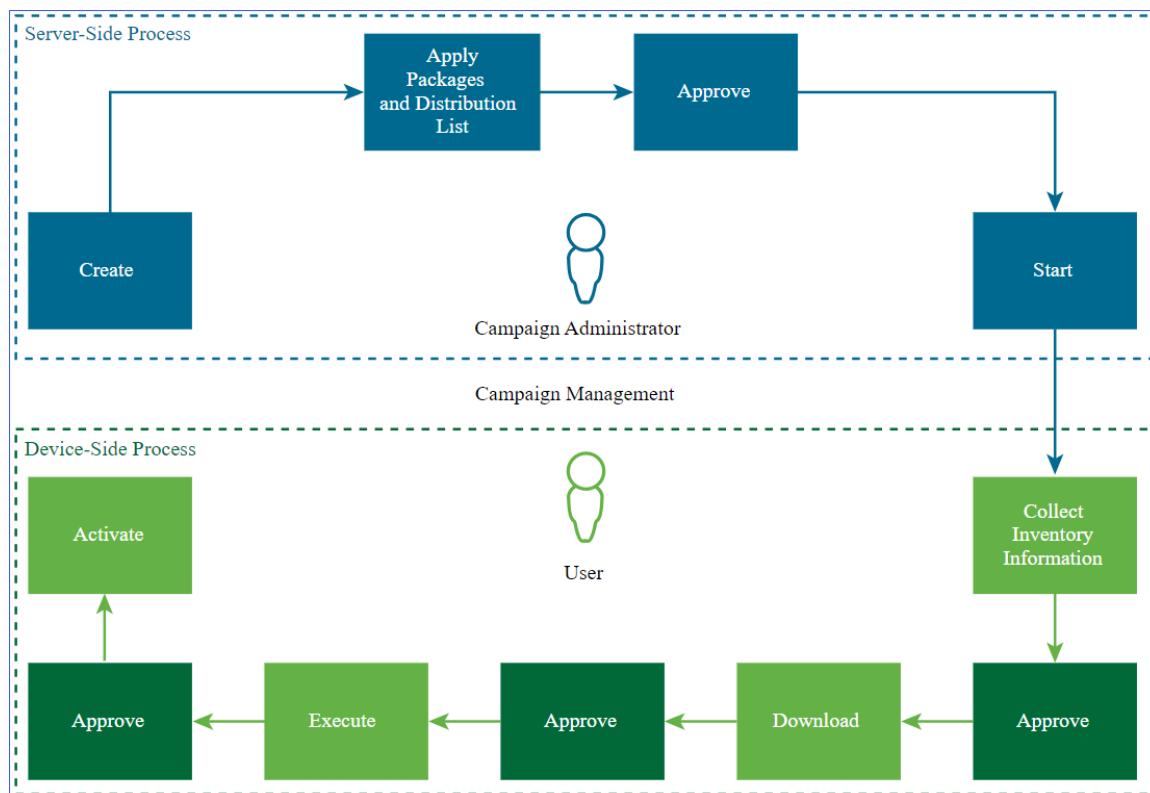
The following use cases describe the campaign approval process:

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:
 - i. View Campaign
 - ii. View Package
 - iii. View Organization Settings
 - iv. View Package
 - v. View Filter Definition
 - vi. 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.

15.3 Campaign State Transition Scheme

The following diagram illustrates the different states of a campaign.



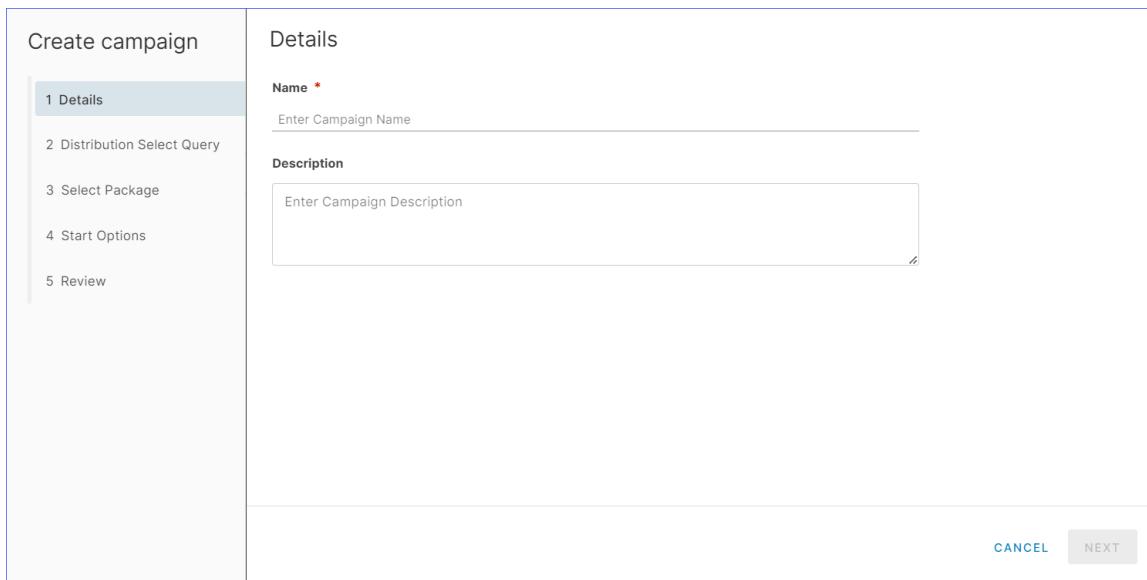
For a headless campaign execution, approvals for downloading, executing, and activating packages are not required.

15.4 Creating a Campaign

To create a campaign in INFER™, perform the following steps:

Create an IoT Package. For information about creating an IoT Package, see "Working with Package Builder" on page 155.

1. From the INFER™ Console, go to **Updates > Campaigns**. The **Updates - Campaigns** page appears.
2. Click **CREATE**. The **Create Campaign** wizard appears as shown below.



The screenshot shows the 'Create campaign' wizard with the 'Details' step selected. On the left, a vertical navigation bar lists steps 1 through 5. Step 1, 'Details', is highlighted. The main area contains fields for 'Name' (with placeholder 'Enter Campaign Name') and 'Description' (with placeholder 'Enter Campaign Description'). At the bottom right are 'CANCEL' and 'NEXT' buttons.

3. Under **Details**, enter a name and under **Description**, enter a brief description for your campaign.
4. Click **NEXT**.
5. 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 device template type:** drop-down, select **GATEWAY** or **THING** to run the campaign on a gateway or a Thing device.



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

3. From **Distribution Select Query** dropdown, select the desired option. Distribution queries are search filter definitions whose results are the devices



on which the campaign runs.

Alternatively, click [+ Create New](#) to create a new distribution query:

- a. From the **Device Template** drop-down, select the type of device template to filter.
- b. From the **Key** drop-down, select the desired metric that you want to filter the devices by. Click [+ADD KEY](#) to create a new key.
- c. Next, from the **Operator** drop-down, 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 and the following action confirmation message appears:



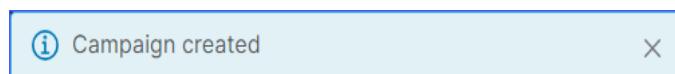
You can also select this query next time you want to create a campaign that requires similar devices to be included.

4. Click **NEXT**.
6. 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**.



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.

7. Under **Start Options**, click the desired option and click **NEXT**.
8. Under **Review**, review your campaign information and click **CREATE**. You have successfully created a campaign, and the following action confirmation message appears:



15.5 Starting the Campaign

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. From the INFER™ Console, go 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 screenshot shows the 'Updates - Campaigns' page in the SmartHub INFER console. On the left is a navigation sidebar with sections like Dashboard, Insights, Inventory, Devices, etc. The main area displays a campaign named 'SafeSpaces01' with a status of 'READY TO START'. Below the basic information, there's a 'Devices' section and a 'Actions' dropdown menu. The 'Actions' menu is open, showing options: Start (highlighted with a red oval), Stop, Approve, Clone, Edit, and Delete. To the right of the campaign details, there's a 'Audit Log' section and a progress bar at the bottom indicating download, execution, and activation completion.

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 **Devices** tab.

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.



15.6 Cloning a Campaign

Cloning a campaign offers several advantages, particularly when you're 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. From the INFER™ Console, go 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.



Else, the existing campaign name will be appended as **Xxxxxxx_clone**

5. Under **Description**, enter a brief description of the new campaign and click **NEXT**.
6. 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 device template type**: drop-down, select **GATEWAY** or **THING** to run the campaign on a gateway or a Thing device.



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

3. From **Distribution Select Query** dropdown, select the desired option. Distribution queries are search filter definitions whose results are the devices on which the campaign runs.

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

- a. From the **Device Template** drop-down, select the type of device template to filter.
- b. From the **Key** drop-down, select the desired metric that you want to filter the devices by. Click **+ADD KEY** to create a new key.
- c. Next, from the **Operator** drop-down, 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 and the following action confirmation message appears:



You can also select this query next time you want to create a campaign that requires similar devices 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**.



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, and the following action confirmation message appears:



15.7 Editing a Campaign

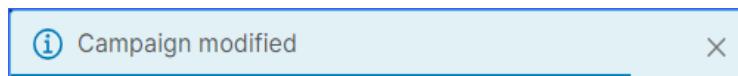
Before you edit a campaign, keep the following conditions in mind:



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. From the INFER™ Console, go 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, and the following action confirmation message appears:



15.8 Deleting a Campaign

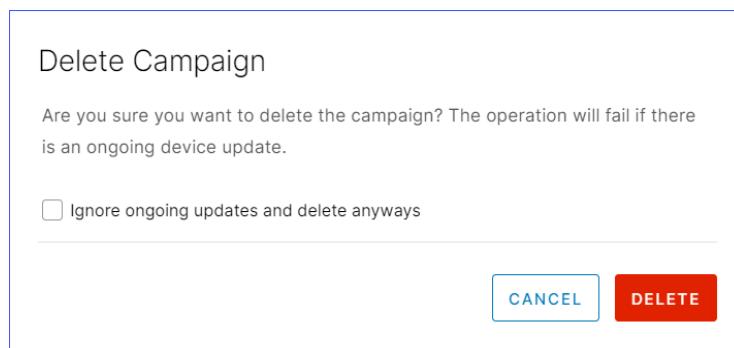
Before you delete a campaign, keep the following condition in mind:



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. From the INFER™ Console, go 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:



4. Click the checkbox if you want to **Ignore ongoing updates and delete anyways**.
5. Click **DELETE**. You have successfully deleted a campaign, and the following action confirmation message appears:

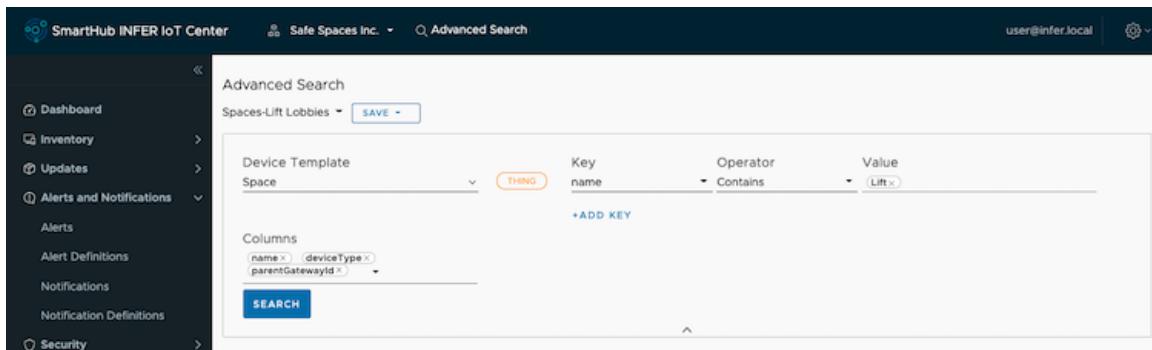


You can stop a campaign only if the devices in the campaign are in a state before the **DOWNLOAD** state.

For more information about Campaign Management APIs, see **Running a Campaign Using Agent SDK** chapter in the INFER™ API Reference Guide.

16 Using Advanced Search

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



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:

- **Device Template**
- **Key:** campaign name campaign state, metric names, device type etc. 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**, **Device Type**, **Location**, and so on. **Device 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.

16.1 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.



- 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 INFER™ Console.

17 Working with Package Builder

This chapter explains the update package, and lists steps to upload and build update packages, using INFER™'s **Packages** sub-module.

17.1 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, and
- Update the devices' BIOS and firmware,
- Run campaigns using Package Builder.

17.2 Building a Package

To build update packages in INFER™, you must have the following Campaign permissions associated with the Organization Administrator Group.



For more information see "Roles and Permissions" on page 3.

- CREATE_PACKAGE
- EDIT_PACKAGE
- DELETE_PACKAGE
- VIEW_PACKAGE



If you are an Advanced user, you can create a package file using the **Package Management CLI** tool. For more information, see "Working with Package Builder" on the previous page.

- From the INFER™ Console, go to **Updates > Packages**. The **Updates - Packages** page appears as shown below:

- Click **BUILDER**. The **Package Builder** wizard appears as shown below:

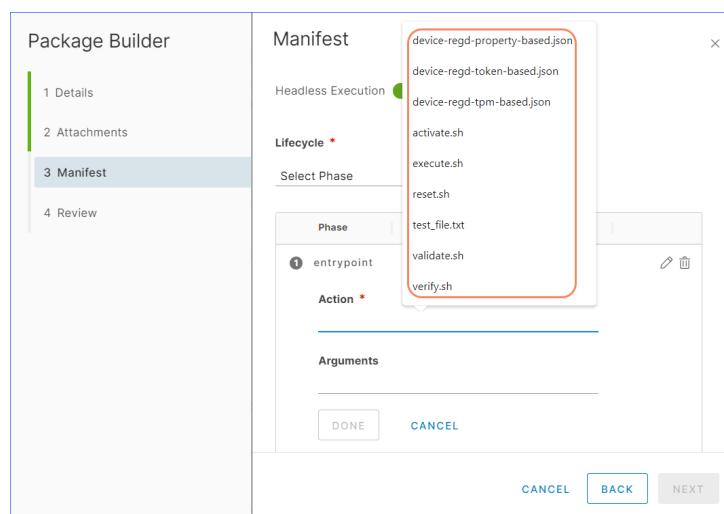
- Under **Name**, enter the new package's name.
- Under **Version**, enter the package's version number.
- Under **Operating system**, select the required OS from the drop down.

6. Next, under **Architecture**, select the required architecture from the dropdown.
7. Under **Description**, enter a brief description of the package.
8. Under **Labels**, enter package-specific keywords to help future searches.
9. Click **NEXT**.
10. Under **Attachments**, click **+ ADD FILES** and browse your local folder and select package files with `*.sh;*.py;*.json;*.ini;*.service;*.txt;*.bin` extensions.
11. Click **NEXT**.
12. Under **Manifest > Headless Execution** appears switched ON by default. This controls the automatic transition of each lifecycle phase without any interaction.
13. Under **Lifecycle**, from the dropdown, select and add the package's desired lifecycle phase.



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.

14. Next, click 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.



When you add lifecycle phases, they are added in the following sequence:

1. **entrypoint**

2. **verify**



3. **execute**

4. **validate**

5. **activate**

6. **reset**



- 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.
- 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.



- For all the executables that are attached for the `action` field, the IoTC 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, and the following action confirmation message appears:



19. The newly created package appears listed as shown below:

Name	Package Id	Version	Operating system	Architecture	Created (IST)	Organization	Labels
Axiom Camera Update	650c19b2608fd3153c20a8b	1.9	linux	amd64	09/21/2023, 3:53 PM	SmartHub	SmartHub, axiom, linux, ...
Air Quality Adapter - test	64f8262a882b4718080a01e0	0.0.1	linux	noarch	09/06/2023, 12:41 PM	SmartHub	
InferZoomRoomAdapter	64f71026882b4718080a01dc	0.0.44	windows	noarch	09/05/2023, 4:55 PM	SmartHub	

Next, 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 INFER™ Console, the file upload and download operations run in the background and the results are displayed 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.



From release 2019.09 onwards, you cannot upload packages to INFER™ using the 2019.07 version of the **Package Management CLI** tool. Ensure that you download the latest version.

18 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.

- The Package File in INFER™ is called *IoTC package*.
- For creating and uploading packages, ensure that you download the latest version of the **Package Management CLI** tool from INFER™.

18.1 Creating a Specification YML File

To create an *IoTC 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 *IoTC package*.

The *package-cli.zip* archive contains the *example-iotc-package* folder. Review the contents in this folder before creating the IoTC 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>/example-
iotc-package/package-source/test_file.txt

- path: <parent directories of build machine>/example-
iotc-package/package-source/verify.sh

- path: <parent directories of build machine>/example-
iotc-package/package-source/execute.sh

- path: <parent directories of build machine>/example-
iotc-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>/example-
iotc-package/package-source/activate.sh

- path: <parent directories of build machine>/example-
iotc-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 with\na 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.

- 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 IoTC Agent is configured with *manifestExecution = ENABLED*, then the campaign runs automatically without any interaction.
- If *headlessExecution* is set to *false* and the IoTC 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 IoTC 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 IoTC Agent. The executable specified for a particular phase is run by the IoTC Agent at each lifecycle phase.
- If the IoTC 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
```

- All the files from the package with relative paths are deployed in a unique directory at the default path that is configured in the IoTC 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/iotc-  
agent/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.

The lifecycle section defines the different lifecycle phases and the corresponding action to take for each phase. For the IoTC Agent to locate an *action* executable after the payload is extracted, and to run the executable, the *actionpath* must match the *installPath* in the *attachments* section.

Or, the *actionpath* 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**



- 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.
- 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.



- For all the executables that are attached for the `action` field, the IoTCAgent 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



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.

18.2 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.

18.3 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.

18.3.1 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/package-
spec.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/package-
spec.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/package-spec.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.yml

For example:

```
cat example-iotc-package/package-spec.yml | ./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
```

18.3.2 Create an IoT Package

Use the following steps to create an IoT 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`.

4. Next, upload the package using the INFER™ Console 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>
```



The upload package command creates the package in the Root organization.

18.3.3 Upload the IoTC Package

This section lists the steps for uploading an IoTC Package.

1. Download and install the **Package Management CLI** tool from INFER™.
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>
```



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 is displayed on the Console.

18.4 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, theINFER™ 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 INFER™ Agent's **DefaultClient** command-line tool.

18.4.1 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 get-
properties --device-id="$camera_id" --type=custom --property-
name="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" --type=custom --property-name="IP"` gets the required properties of the IP camera such as IP address using the IP camera ID.

```

curl http://$camera_ip/cgi/UpdateFirmware
filename=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
```

19 Controlling a Campaign 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 INFER™ micro services for every `commandFetchIntervalSeconds` expiry.
- You can configure the property value through the **Device Template** tab in the INFER™ 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 INFER™ Server by calling the `get-command` every 30 seconds.



For each lifecycle phase, the IoTCAgent receives a command from the Server to perform the download, execute, and activate operations.

19.1 Running a Campaign using Default Properties

Run an OTA update for the IoTCAgent using default properties by performing the following steps:



-
1. Using the [Package Builder](#) or the [Package Management CLI](#) tool:
 - a. Create an IoT Package.
 - b. Upload the IoT Package to the repository. Alternatively, you can use the Console to upload to the repository. For more information about uploading the IoT Package, see [Upload the IoT Package](#).
 2. Enroll devices.
 3. Create a campaign using a distribution select query and the packages that you uploaded while creating the campaign.
 4. Start the campaign.

The IoTAgent 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.

19.2 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 [Package Builder](#) or the [Package Management CLI](#) tool, perform the following steps:
 - a. Create an IoT Package.
 - b. Upload the IoT Package to the repository. Alternatively, use the INFER™ 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 IoTAgent 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.

19.2.1 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 --campaign-id=<campaign id>

DefaultClient schedule --type=download --campaign-id=<campaign id> --start-time=0 --end-time=0

DefaultClient schedule --type=download --campaign-id=<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> --campaign-id=<campaign Id> [--start-time=<start time window> --end-time=<end time window>]
```

For example:



```
DefaultClient schedule --type=execution --campaign-id=<campaign id>

DefaultClient schedule --type=execution --campaign-id=<campaign id> --start-time=0 --end-time=0

DefaultClient schedule --type=execution --campaign-id=<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> --campaign-id=<campaign Id> [--start-time=<start time window> --end-time=<end time window>]
```

For example:

```
DefaultClient schedule --type=activation --campaign-id=<campaign id>

DefaultClient schedule --type=activation --campaign-id=<campaign id> --start-time=0 --end-time=0

DefaultClient schedule --type=activation --campaign-id=<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.



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**

19.3 Running a Campaign in Headless Mode

This section lists the prerequisites for running a campaign for the IoT Agent in Headless Mode.

- Run the IoTCAgent 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 IoTCAgent. The `get-commands` calls from the IoT Agent listens to the Campaign commands and the campaign downloads, executes, and activates updates.

19.3.1 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`.

19.4 Approving the 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 INFER™ Console. To view the progress of the campaign, select the campaign from the list and click the **Devices** tab.



The default interval for the IoTCAgent to fetch new commands from the Server is 30 seconds. You can change the interval value through the Device 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=<campaign Id>
```



Copy the campaign ID from the Campaigns page of the INFER™ Console.

- After the campaign reaches the **Waiting For Execution Approval** state:

```
DefaultClient schedule --type=execution --campaign-id=<campaign Id>
```

- After the campaign reaches the **Waiting For Activation Approval** state:

```
DefaultClient schedule --type=activation --campaign-id=<campaign Id>
```

20 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.

20.1 What is an Alert?

An alert is a specific instance in time logged by INFER™ when a device meets the context and conditions specified in an alert definition.

- **Purpose:** Alerts in INFER™ 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 from INFER™ 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.

20.1.1 Device Offline Alerts

You can create alert definitions on device templates to trigger an alert when a device does not ingest any metrics for a particular time duration.



For a newly added device that does not have any ingested metrics, at least two data points must be ingested before the absence of more metrics triggers a **Device Offline** alert.

20.1.2 Searching Alerts

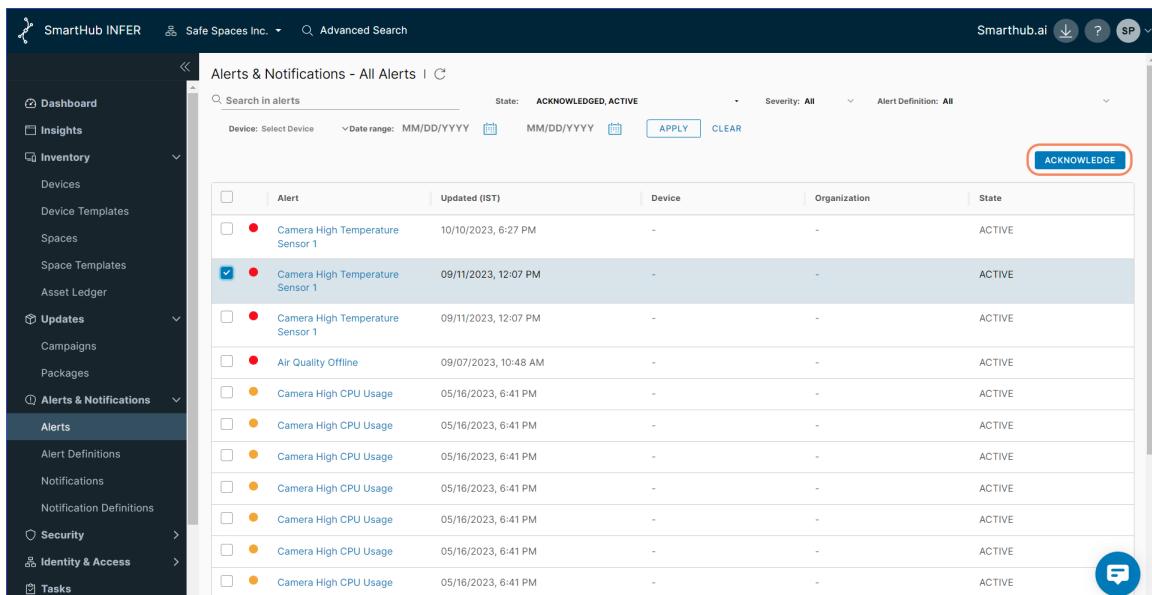
From the **Alerts and Notifications > Alerts** tab, you can search for alerts:

- by their definition,
- by the update time range, and
- by their states: **ACTIVE**, **ACKNOWLEDGED**, or **CANCELED**.

20.1.3 Acknowledging Alerts

To acknowledge an active alert from the list of alerts, select the alert and click **ACKNOWLEDGE**. The alert's state changes to **Acknowledged** and the user name of the person who acknowledged the alert is displayed.

You can also acknowledge alerts from the following tab:



The screenshot shows the SmartHub INFER interface with the 'Alerts & Notifications - All Alerts' tab selected. The table lists various alerts, including 'Camera High Temperature Sensor 1' which is currently selected. The 'ACKNOWLEDGE' button for this specific alert is highlighted with a red box. Other alerts listed include 'Air Quality Offline', multiple 'Camera High CPU Usage' events, and 'Camera High Temperature Sensor 1' again.

Alert	Updated (IST)	Device	Organization	State
Camera High Temperature Sensor 1	10/10/2023, 6:27 PM	-	-	ACTIVE
Camera High Temperature Sensor 1	09/11/2023, 12:07 PM	-	-	ACTIVE
Camera High Temperature Sensor 1	09/11/2023, 12:07 PM	-	-	ACTIVE
Air Quality Offline	09/07/2023, 10:48 AM	-	-	ACTIVE
Camera High CPU Usage	05/16/2023, 6:41 PM	-	-	ACTIVE
Camera High CPU Usage	05/16/2023, 6:41 PM	-	-	ACTIVE
Camera High CPU Usage	05/16/2023, 6:41 PM	-	-	ACTIVE
Camera High CPU Usage	05/16/2023, 6:41 PM	-	-	ACTIVE
Camera High CPU Usage	05/16/2023, 6:41 PM	-	-	ACTIVE
Camera High CPU Usage	05/16/2023, 6:41 PM	-	-	ACTIVE
Camera High CPU Usage	05/16/2023, 6:41 PM	-	-	ACTIVE

20.1.4 Alert History

You can view the alert history of a device and know if an alert is new or an existing one.

You can also know the:

- number of times the device has raised this alert,
- identify the metric, value, and
- the time stamp when the alert was triggered.

Select the alert definition and click the **History** tab. A graph indicating the alert states is also displayed.

Alert Notifications are sent only if notifications are configured correctly. They are sent for both **ACTIVE** and **CANCELLED** states.

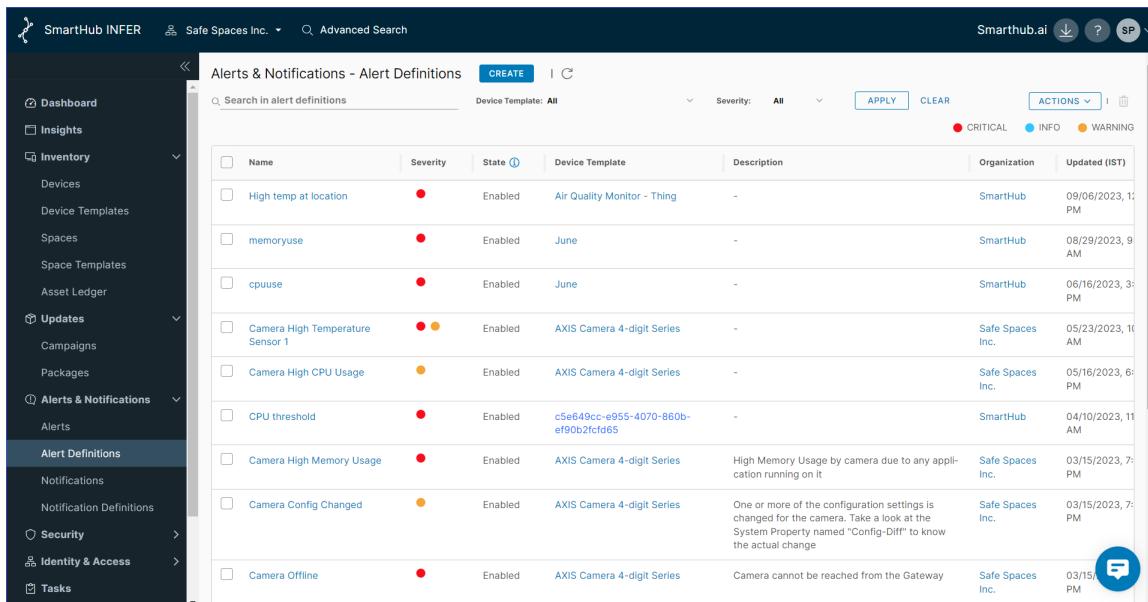
20.2 What is an Alert Definition?

An alert definition is a set of conditions necessary to trigger an alert as explained in "What is an Alert?" on page 183. Alert definitions are a combination of symptoms and recommendations that you combine to identify problem areas and generate alerts.

Alert definitions consist of:

- a device template,
- a device metric/property,
- a condition expression, and
- the number of times the condition must be true for a device to trigger that alert.

For example, you can define an alert to trigger whenever the temperature of a device 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.



The screenshot shows the SmartHub INFER interface with the 'Alert Definitions' section selected in the sidebar. The main view displays a table of alert definitions with columns for Name, Severity, State, Device Template, Description, Organization, and Updated (IST). The table lists several alerts, such as 'High temp at location', 'memoryuse', 'cpuuse', and various camera-related alerts like 'Camera High Temperature Sensor 1' and 'Camera Config Changed'. Each alert entry includes a checkbox, a severity indicator (red for Critical, yellow for Info, orange for Warning), and a status (Enabled). The 'Severity' dropdown is set to 'All'. The 'Organization' column shows entries like 'SmartHub' and 'Safe Spaces Inc.'. The 'Updated (IST)' column shows dates and times for each alert's last update.

Name	Severity	State	Device Template	Description	Organization	Updated (IST)
High temp at location	CRITICAL	Enabled	Air Quality Monitor - Thing	-	SmartHub	09/06/2023, 1: PM
memoryuse	CRITICAL	Enabled	June	-	SmartHub	08/29/2023, 9 AM
cpuuse	CRITICAL	Enabled	June	-	SmartHub	06/16/2023, 3: PM
Camera High Temperature Sensor 1	CRITICAL	Enabled	AXIS Camera 4-digit Series	-	Safe Spaces Inc.	05/23/2023, 10 AM
Camera High CPU Usage	WARNING	Enabled	AXIS Camera 4-digit Series	-	Safe Spaces Inc.	05/16/2023, 6: PM
CPU threshold	CRITICAL	Enabled	c5e649cc-e955-4070-860b-ef90b2f9fd65	-	SmartHub	04/10/2023, 11 AM
Camera High Memory Usage	CRITICAL	Enabled	AXIS Camera 4-digit Series	High Memory Usage by camera due to any application running on it	Safe Spaces Inc.	03/15/2023, 7: PM
Camera Config Changed	WARNING	Enabled	AXIS Camera 4-digit Series	One or more of the configuration settings is changed for the camera. Take a look at the System Property named "Config-Diff" to know the actual change	Safe Spaces Inc.	03/15/2023, 7: PM
Camera Offline	CRITICAL	Enabled	AXIS Camera 4-digit Series	Camera cannot be reached from the Gateway	Safe Spaces Inc.	03/15/2023, 7: PM

20.3 Creating an Alert Definition

This section lists the various alert definition types you can create using the Alerts module in INFER™.

- A. **Creating an Alert Definition across multiple device templates:** You can create a single alert definition that works across multiple device templates. When you create alert definitions for multiple device templates, ensure that the metrics or properties for the alert definition symptom is common across all the device templates that you have selected.
- B. **Creating an alert definition for single device template with command definition (with arguments):** You can create an alert definition for a single device template and select command definition (with arguments) that is executed when the alert is triggered.
- C. **Creating an Alert Definition for devices in an Advanced Search Query:** If you have saved an advanced search query for devices, you can create an alert definition for those devices that are part of that saved query.
- D. **Creating a Threshold Alert Definition:** You can also create a threshold alert definition for a single device template or across multiple device templates from the INFER™ Console.
- E. **Creating an Offline Alert Definition:** You can create an offline alert definition from the INFER™ Console to trigger device offline alerts if the INFER™ Server does not receive metrics or system property values for a specified duration.

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:



For more information see "Introduction" on page 1.

1. From the INFER™ Console, go to **Alerts & Notifications > Alert Definitions**.
2. Click **CREATE**. The Create Alert Definition wizard appears as shown below:

<p>Create Alert Definition</p> <p>1 Details</p> <p>2 Devices</p> <p>3 Condition</p> <p>4 Recommendation</p> <p>5 Notification</p> <p>6 Commands</p> <p>7 Review</p>	<p>Details This step consists of basic details of the Alert definition</p> <p>Name * CPU Temp@45 degrees</p> <p>Description Tracks CPU Temperature beyond 45 degrees</p> <p style="text-align: right;">CANCEL NEXT</p>
--	---

3. Under **Details**, enter a **Name** and **Description** of your alert.
 4. Click **NEXT**.
 5. Under **Select Devices > TEMPLATES**, select one or more device templates.
 - You can create a single alert definition that works across multiple device 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 device templates that you have selected.
 6. Next, click **SAVED SEARCH**. Use the **Select** drop-down to search for previously searched device templates.
- 
If you have a saved advanced search query for devices, you can create an alert definition for those devices that are part of the query.
7. Click **PREVIEW** to review values of the selected device template.
 8. Click **NEXT**.
 9. Under **Condition**, choose between setting up **THRESHOLD** and **OFFLINE** alert definitions.
 - Threshold alert definition is defined by a trigger condition on Metric/Property.
 - Offline alert definition is defined by time interval.



-
10. Under **THRESHOLD > Symptom**, from the drop-downs, add conditions that trigger your alert by selecting the values for **Metric/Property**, **Condition**, **Severity**, and **Trigger Count**.

- Threshold alert definition is defined by a trigger condition on Metric/Property.



- You can create a threshold alert definition for a single device template or across multiple device templates.
- Ensure that the selected metric or property exists on all selected device templates.

11. Under **Symptom**, select a metric or system property, its condition, and enter the metric value to trigger the alert.



- 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

12. From the **Severity** drop-down, select the severity of the alert:

The alert severity types are:



- **CRITICAL - Red**
- **WARNING - Orange**
- **INFO - Blue**
- **NORMAL** - Defines the normal threshold for the alert to cancel.

13. Click **+ Add** to add multiple conditions and severity options to the symptom.
14. From the **Trigger Count** drop-down, select the number of times the condition must be met to trigger the alert.
-
- 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.

15. Next, click **OFFLINE**.

- You can trigger device offline alerts if the INFER™ Server does not receive metrics or system property values for a specified duration.
- You can create device offline alert definitions only for the allowed metrics that are on the device template.
- Offline alert definition is defined by time interval.

16. Under **Check interval for absence of metrics or system properties**, enter the duration in minutes that the INFER™ Server must wait to receive metrics and system property values from a device before triggering the alert.

17. Under **Recommendation**, enter the action that the technician or administrator must take when the alert is triggered.

18. Click **NEXT**.

19. Under **Notification**, click **Enable Notifications** switch to send a notification when the alert is triggered.

20. Under **Select Notification**, from the drop-down, select the **Notification** that will be sent when the Alert is triggered.

21. Click **NEXT**.

22. Under **Commands**, click **Enable Commands** switch to select the commands that will be executed when the alert is triggered.

23. Next click **+ Add** and select the desired command from the drop-down.

24. Specify the parameters under **Argument Name** and **Argument Value**.

25. Click **DONE**.

26. Click **NEXT**.

27. Under **Review**, review the new alert definition information you entered and click **SAVE**. You have successfully created a new alert definition, and the following action confirmation message appears:



20.4 Editing an Alert Definition

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.

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:



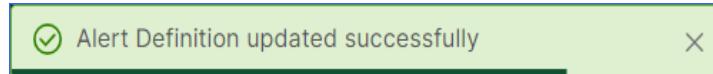
For more information see "Introduction" on page 1.

1. From the INFER™ Console, go to **Alerts & Notifications > Alert Definitions**.
 2. From the listed alert definitions, click the alert definition which you desire to edit.
- The following tab appears as shown below:

The screenshot shows the SmartHub INFER interface. On the left, there's a navigation sidebar with various sections like Dashboard, Insights, Inventory, Updates, and Alerts & Notifications. Under Alerts & Notifications, 'Alert Definitions' is selected. The main area displays a list of alert definitions with columns for Name and Severity. One alert, 'CPU Temp@45 degrees', has a blue severity indicator. Another, 'High CO2 at location', has an orange severity indicator. The alert 'Camera High Temperature Sensor 1' is selected, and its details are shown in a modal window on the right. The modal includes fields for Alert Definition State (Enabled), Device Template (AXIS Camera 4-digit Series), and a Symptom table. The Symptom table lists 'Temperature_SO > 80' as CRITICAL and 'Temperature_SO > 50' as WARNING. Below the table, it shows a Trigger Count of 1, a Recommendation to 'Reboot the camera', and a Notification to 'SmartHub Operations Team (SHOT)'. At the top of the modal, there's an 'Edit' button highlighted with a red circle.

3. Under **Actions** drop-down as highlighted above, click**Edit**.
4. The **Edit Alert Definition** wizard is displayed.

-
5. Edit the existing alert definition details and click **SAVE**. You have successfully edited an alert definition, and the following action confirmation message appears:



If you change the **Condition** of your alert definition, all active alerts from the previous condition are automatically canceled.

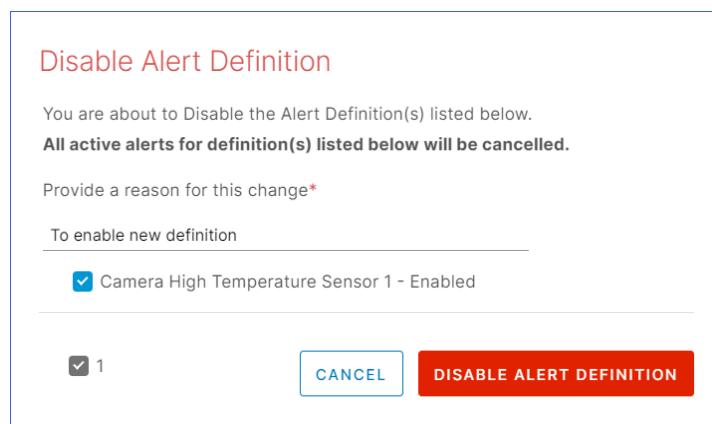
20.5 Disabling an Alert Definition

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:



For more information see "Introduction" on page 1.

1. From the INFER™ Console, go to **Alerts & Notifications > Alert Definitions**.
2. From the listed alert definitions, click the enabled alert definition which you desire to disable.
3. Under **Actions** drop-down, click**Disable**.
4. The **Disable Alert Definition** pop-up appears as shown below:

A modal dialog box titled "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

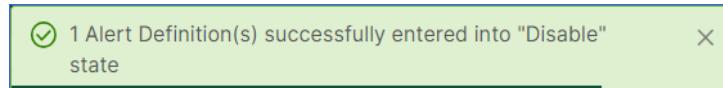
1

CANCEL **DISABLE ALERT DEFINITION**

The dialog has a light blue border and a white background. The "DISABLE ALERT DEFINITION" button is highlighted with a red background and white text.



-
5. Enter the reason for the change and click **DISABLE ALERT DEFINITION**. You have disabled the alert definition successfully, and the following action confirmation message appears:



If you change the condition of your alert definition, all active alerts from the previous condition are automatically canceled.

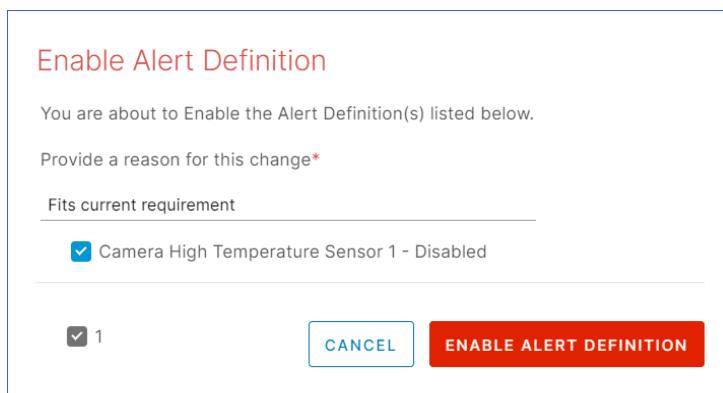
20.6 Enabling an Alert Definition

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:

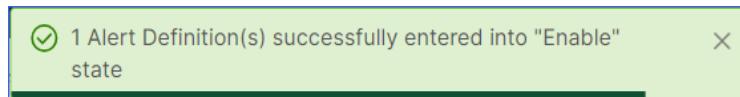


For more information see "Introduction" on page 1.

1. From the INFER™ Console, go to **Alerts & Notifications > Alert Definitions**.
2. From the listed alert definitions, click the disabled alert definition which you desire to enable.
3. Under **Actions** drop-down, click**Enable**.
4. The **Enable Alert Definition** pop-up appears as shown below:



-
5. Enter the reason for the change and click **ENABLE ALERT DEFINITION**. You have enabled the alert definition successfully, and the following action confirmation message appears:



20.7 What is a Notification?

The Notifications module enables you to receive timely notifications without logging in to the INFER™, or without providing an integration point into the existing monitoring systems.

The Notifications module acts as a primary interface for all HTTP and email (SMTP) notifications from the INFER™ Server. All the other INFER™ services communicate with the notifications service to send notifications to the external servers.

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.

- **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 displayed 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.



20.7.1 Viewing Notifications

You can use the Notifications tab as shown below to view email and REST notifications.

To view notifications in INFER™, you must have the VIEW_NOTIFICATION_INSTANCE permission associated with the Organization Administrator Group, and perform the following steps:



For more information see "Introduction" on page 1.

- From the INFER™ Console, go to **Alerts & Notifications** > **Notifications**. The **Alerts & Notifications - Notifications** page appears as shown below:

2. Click the desired notification to view more information about it.

20.8 What is a Notification Definition?

Notifications are email and REST alerts that inform users or other parts of a system about important events, updates, or changes.

Notification Definitions outline the format, content, and behavior of these notifications. A Notification Definition typically refers to a description or specification of how notifications should be structured and delivered within INFER™.

Notification definitions contain details such as the:

- a notification's destination,
- the sender, and
- the number of times to retry sending.

20.9 Creating a Notification Definition

This section lists the steps to create a notification definition from the INFER™.

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:



For more information see "Introduction" on page 1.

1. From the INFER™ Console, go to **Alerts & Notifications > Notification Definitions**.
2. Click **CREATE**. The **Create Notification Definition** wizard appears as shown below:

<p>Create Notification Definition</p> <p>1 Details</p> <p>2 Settings</p> <p>3 Recurrence</p> <p>4 Review</p>	<p>Details This step consists of basic details of the notification definition</p> <p>Name * Notification Definition Name</p> <p>Description Description</p> <p style="text-align: right;">CANCEL NEXT</p>
--	--

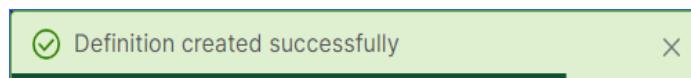
3. Under **Name**, enter a name for your alert.
4. Under **Description**, enter a brief description of your alert.



-
5. Click **NEXT**.
 6. Under **Settings > Type**, from the drop-down, choose the notification type.

20.9.1 Email Notification

7. In step 6. if you chose **Email Notification**, under **Notification Categories**, from the drop-down, choose your desired notification category.
8. Under **Advanced Settings**, the fields carry default values. However, these can be overwritten. You can revert to default values by deleting the overwritten values.
9. Enter the values for **Sender Name**, **Base URL**, **Sender Email Address**, and **Email Subject**.
10. Under --Insert field--, use the drop-down to select the desired option.
11. Click **NEXT**.
12. To configure your notification to reoccur, under **Recurrence**, click the checkbox against **Recurrence notification**
13. Under **Recurrence Interval**, specify the **days**, **hours**, and **minutes**.
14. To configure the maximum number times the notification has to reoccur, under **Max Recurrence Count**, enter between 1 - 100 recurrence count.
15. Click **NEXT**.
16. Under **Review**, review the notification definition information you entered and click **SAVE**. You have successfully created a new notification definition, and the following action confirmation message appears:



20.9.2 REST Notification

17. In step 6. if you chose **REST Notification**, under **Notification Categories**, from the drop-down, choose your desired notification category.
18. Click the checkbox against **Secure Protocol (Secure (TLS) is recommended)**
19. Under **Host URL**, enter the host URL.



The default port number is 443.

20. Under **Certificate**, paste the certificate details.
21. Under **Authentication Type > Basic**, from the drop-down, select your desired authentication type.



Auth-based REST Server is recommended.

22. Under **Basic**, enter the Username and Password.
23. Under **Advanced**, if required, click the checkbox against **Retry Schedule**.
24. Under **Retry Interval**, specify the **hours**, **minutes**, and **Seconds**.
25. Under **Request Timeout**, specify the **minutes**, and **Seconds**.
26. Under **Max Retry Count**, specify the retry count.
27. Under **Headers**, click [+ Add New Header](#) to add a new header.
28. Specify the **Header Name** and **Header Value** parameters, and click **DONE**.
29. Next, click the checkbox against **Use Default Rest Template** to use the default REST Template.
30. Else, under **Body Template**, edit the desired values.
31. Under **--Insert field--**, use the drop-down to select the desired option.
32. Under **Validate Response**, enter the response string.
33. Click **NEXT**.
34. Under **Link**, setup linked notifications for sent notifications.
35. Under **On success, send additional notification**, from the drop-down, select the desired option.
36. 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.



-
37. 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.
 38. Click **NEXT**.
 39. Under **Review**, review the notification definition information you entered and click **SAVE**. You have successfully created a new notification definition, and the following action confirmation message appears:



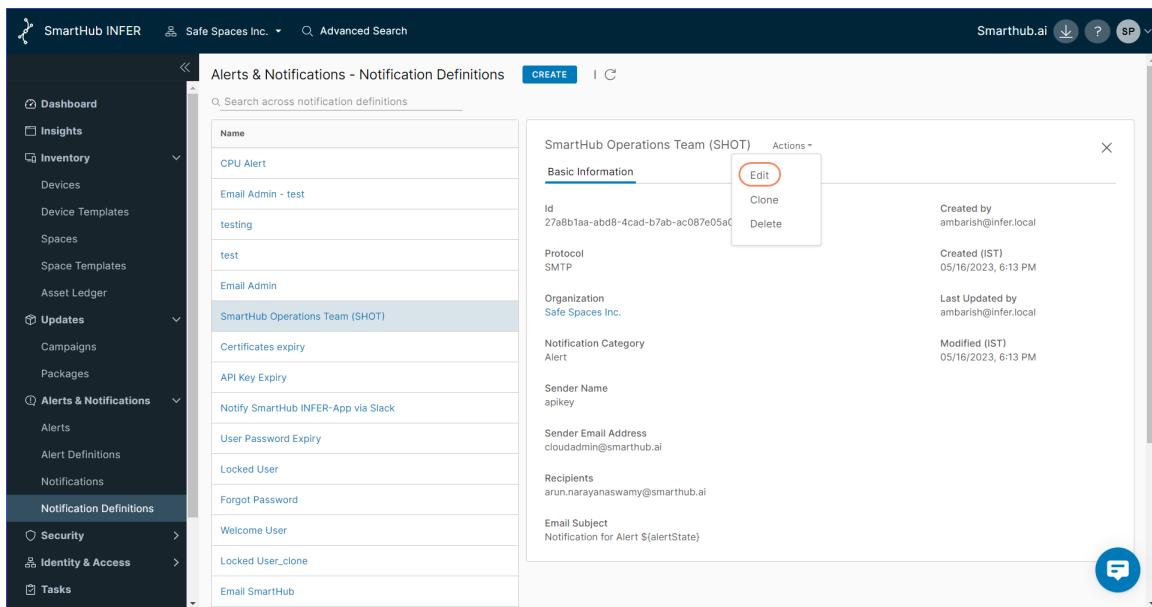
20.10 Editing a Notification Definition

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:



For more information see "Introduction" on page 1.

1. From the INFER™ Console, go to **Alerts & Notifications > Notification Definitions**.
2. From the listed notification definitions, click the notification definition which you desire to edit. The following tab appears as shown below:



The screenshot shows the SmartHub INFER interface. On the left, there's a navigation sidebar with various sections like Dashboard, Insights, Inventory, Updates, and Alerts & Notifications. Under Alerts & Notifications, 'Notification Definitions' is selected. In the main area, a table lists several notification definitions. One row, 'SmartHub Operations Team (SHOT)', is highlighted in blue. To its right, a detailed view is shown with fields for Basic Information (Id: 27a8b1aa-abd8-4cad-b7ab-ac087e05a0, Protocol: SMTP, Organization: Safe Spaces Inc., Category: Alert), Sender details (Name: apikey, Email: clouadmin@smarthub.ai), Recipients (arun.narayanaswamy@smarthub.ai), and Email Subject (Notification for Alert \${alertState}). An 'Actions' dropdown menu is open next to the organization name, with 'Edit' highlighted and circled in red.

- Under **Actions** drop-down as highlighted above, click**Edit**. The **Edit Notification Definition** wizard appears.



Type and **Notification Categories** parameters are not editable.

- Edit the notification definition details and click **SAVE**. You have successfully edited a notification definition, and the following action confirmation message appears:



20.11 Cloning a Notification Definition

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:



For more information see "Introduction" on page 1.

- From the INFER™ Console, go to **Alerts & Notifications > Notification Definitions**.

-
2. From the listed notification definitions, click the notification definition which you desire to clone.
 3. Under **Actions** drop-down, click **Clone**. The **Create Notification Definition** wizard appears.



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, and the following action confirmation message appears:



20.12 Deleting a Notification Definition

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:



For more information see "Introduction" on page 1.

1. From the INFER™ Console, go to **Alerts & Notifications > Notification Definitions**.
2. From the listed alert definitions, click the enabled alert definition which you desire to disable.
3. Under **Actions** drop-down, click **Disable**.
4. The **Delete Notification Definition** pop-up appears as shown below:

Delete Definition

This notification definition might be in use in an alert definition or a campaign.
Are you sure you want to delete ?

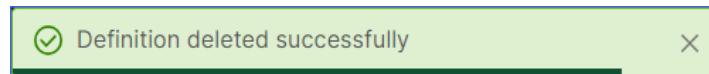
Definition Name : CPU Alert

CANCEL DELETE



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, and the following action confirmation message appears:



21 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.



INFER™ sends an email notification to API Key owners 14 days, 7 days, and 1 day before the token's expiration date.

21.1 Creating a Key

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:



For more information see "Roles and Permissions" on page 3.

1. From the INFER™ Console, go to **Identity & Access > API Keys**. The **Identity & Access - API Keys** page is displayed.
2. Click **CREATE**. The **Create API Key** wizard appears.

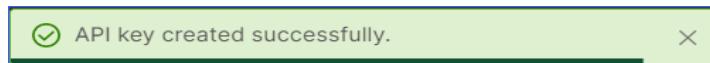


3. Under **Display Name** enter the display name of the new key.
4. Under **API Key Name**, enter the name of the new key.



Spaces and special characters are not allowed.

5. Under **Email Address**, enter the email address.
6. Under **Token Expiry In Days**, enter a value between 30 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, 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:



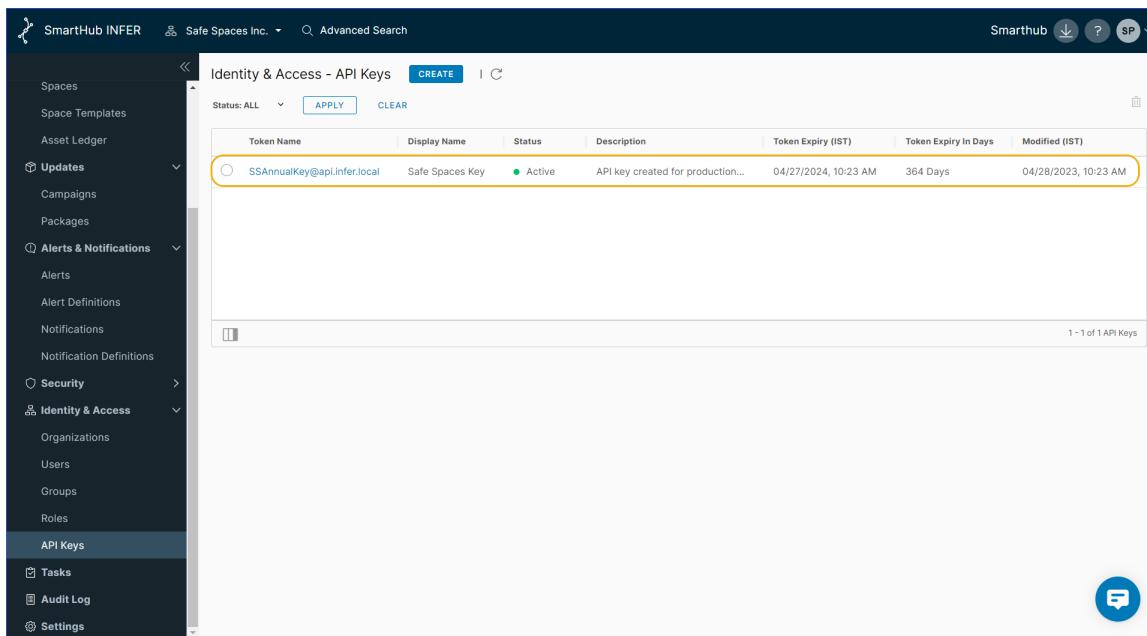
API Key Token

Token **SSAnnualKey (Safe Spaces Key)** successfully created,
Would expire on 04/27/2024, 10:23 AM
Please copy the token now, **This token would not be displayed again**

eyJraWQiOilwMGIwYWI1NC02Nzc1LTQzNDgtODgxNS0xNzE2ZjRhNGZl

DONE

11. Click 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)
SSAnnualKey@api.infer.local	Safe Spaces Key	Active	API key created for production...	04/27/2024, 10:23 AM	364 Days	04/28/2023, 10:23 AM



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.

21.2 Editing a Key

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:



For more information see "Roles and Permissions" on page 3.

1. From the INFER™ Console, go to **Identity & Access > API Keys**. The **Identity & Access - API Keys** page is displayed.
2. Click the desired key. The details of the key are displayed.
3. From the **Actions** drop-down, 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, and the following action confirmation message appears:



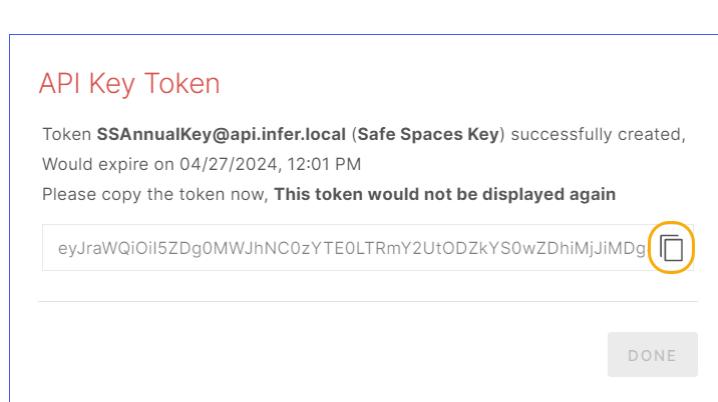
21.3 Renewing a Key

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:



For more information see "Roles and Permissions" on page 3.

1. From the INFER™ Console, go to **Identity & Access > API Keys**. The **Identity & Access - API Keys** page is displayed.
2. Click the desired key. The details of the key are displayed.
3. From the **Actions** drop-down, 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 action confirmation message and **API Key Token** pop-up appear:



-
6. Click  to copy the token to the clipboard.
 7. Click **DONE**. The page defaults to the **Identity & Access > API Keys** page.

However, all the above Key states can be brought to **Renewed** during the following circumstances:

- To ensure uninterrupted business operations, during key creation, users can also create an extra backup key.
- Additionally, when the existing key is nearing its expiry date, users can replace it with their backup key before existing key's expiry. In this case, the replaced key gets the **Revoked** status.

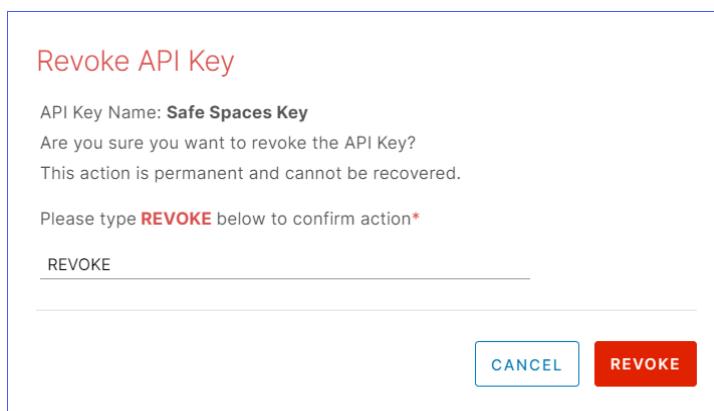
21.4 Revoking a Key

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:



For more information see "Roles and Permissions" on page 3.

1. From the INFER™ Console, go to **Identity & Access > API Keys**. The **Identity & Access - API Keys** page is displayed.
2. Click the desired key. The details of the key are displayed.
3. From the **Actions** drop-down, click **Revoke**. The **Revoke API Key** pop-up appears as shown below:



The pop-up window has a light blue border and contains the following text and fields:

Revoke API Key

API Key Name: **Safe Spaces Key**

Are you sure you want to revoke the API Key?
This action is permanent and cannot be recovered.

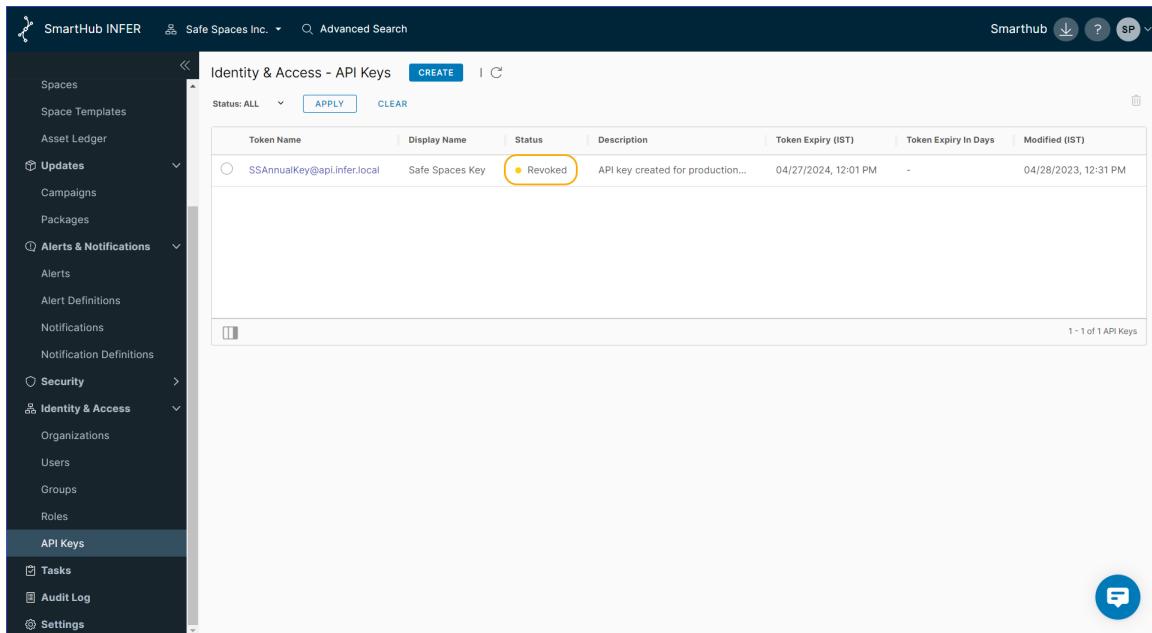
Please type **REVOKE** below to confirm action*

CANCEL **REVOKE**

4. Type **REVOKE** and click **REVOKE**. You have successfully updated a key, and the following action confirmation message appears:



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)
SSAnnualKey@api.infer.local	Safe Spaces Key	Revoked	API key created for production...	04/27/2024, 12:01 PM	-	04/28/2023, 12:31 PM

21.5 Deleting a Key

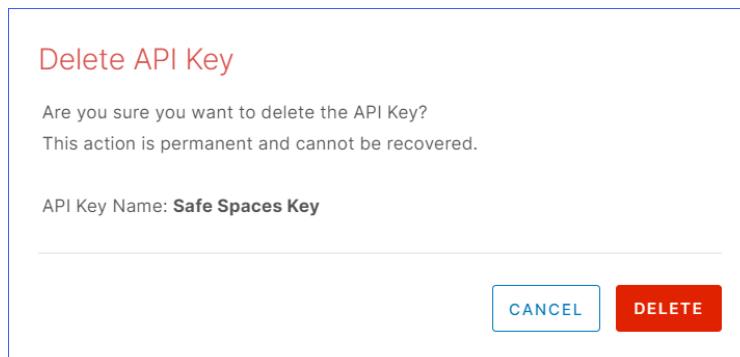
To delete an API Key in INFER™, you must have the **DELETE_API_KEY** permission associated with the Organization Administrator Group, and perform the following steps:



For more information see "Roles and Permissions" on page 3.

1. From the INFER™ Console, go to **Identity & Access > API Keys**. The **Identity & Access - API Keys** page is displayed.

-
2. Click the desired key. The details of the key are displayed.
 3. From the **Actions** drop-down, click **Delete**. The **Delete API Key** pop-up appears as below:



4. Click **DELETE**. You have successfully updated a key, and the following action confirmation message appears:



21.6 Viewing Key Details

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:



For more information see "Roles and Permissions" on page 3.

1. From the INFER™ Console, go to **Identity & Access > API Keys**. The **Identity & Access - API Keys** page is displayed.
2. Click the desired key. The details of the key are displayed as shown below:

Identity & Access - API Keys

SafeSpacesInc (363 Days) 		ACTIVE	Actions ▾
Basic Information Permissions History			
Display Name	SafeSpacesInc		
Token Name	SafeSpacesInc@api.infer.local		
Token Expiry (IST)	04/26/2024, 3:17 PM		
Email Address	admin@ssi.com		
Description	Production key to interoperate with INFER		
Organization	Safe Spaces Inc.		
Id	8c5ff4d2-ae1d-466c-bb31-7c716d45b9f2		
Created (IST)	04/28/2023, 3:17 PM		
Created by	suraj.panicker@infer.local		
Modified (IST)	04/28/2023, 3:17 PM		



21.7 Viewing Key Permissions

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:



For more information see "Roles and Permissions" on page 3.

1. From the INFER™ Console, go to **Identity & Access > API Keys**. The **Identity & Access - API Keys** page is displayed.
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.

21.8 Viewing Key History

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:



For more information see "Roles and Permissions" on page 3.

1. From the INFER™ Console, go to **Identity & Access > API Keys**. The **Identity & Access - API Keys** page is displayed.
2. Click the desired key.
3. Click **History** tab to view the history of this key.

21.9 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.

22 Settings

The **Settings** module allows INFER™ 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.

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.



For more information see "Roles and Permissions" on page 3.

- A. Custom branding
- B. Default gateway template
- C. Default thing template
- D. Audit log retention period
- E. External identity provider (SAML/LDAP)
- F. Default Insights dashboard
- G. Notifications
- H. Notification definitions
- I. System notifications
- J. Enable approvals for OTA campaign permission

22.1 Setting up Custom Branding

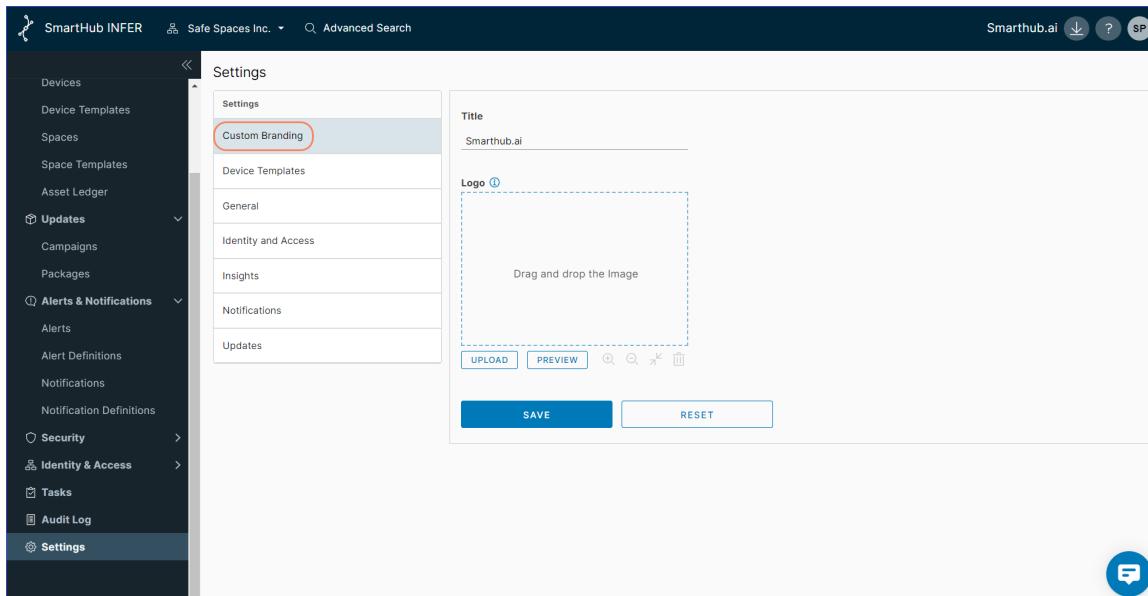
Consistency in branding across all touch-points helps create a cohesive and memorable brand experience for your customers.

The Custom Branding module in INFER™ is a powerful tool to customize the visual identity and appearance of INFER™ to align with your organization's broader brand identity.

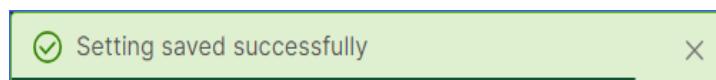
The Settings module in INFER™ helps to promote your organization's brand recognition, building trust with your customers, and highlight the values and personality of your organization's brand.

To create a new custom brand in INFER™, perform the following steps:

1. From the INFER™ Console, go to **Settings**. The **Custom Branding** tab appears selected by default as shown below:



2. Under **Title**, enter your organization's name.
3. Under **Logo**, drag/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, and the following action confirmation message appears:



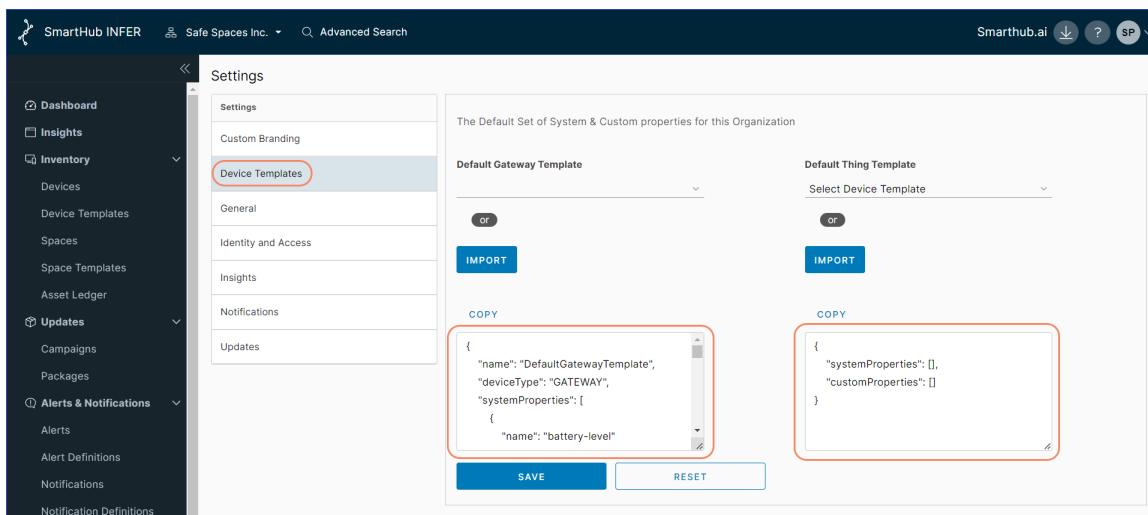
7. Click **RESET** to revert to default settings.

22.2 Setting up the Default Gateway & Thing Template

The Settings module in INFER™ 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. From the INFER™ Console, go to **Settings > Device Templates**. This tab appears as shown below:



```

{
  "name": "DefaultGatewayTemplate",
  "deviceType": "GATEWAY",
  "systemProperties": [
    {
      "name": "battery-level"
    }
  ]
}

```

```

{
  "systemProperties": [],
  "customProperties": []
}

```

2. Under **Default Gateway Template**, use the drop-down to select the 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.

22.3 Setting up Audit Log Retention Period

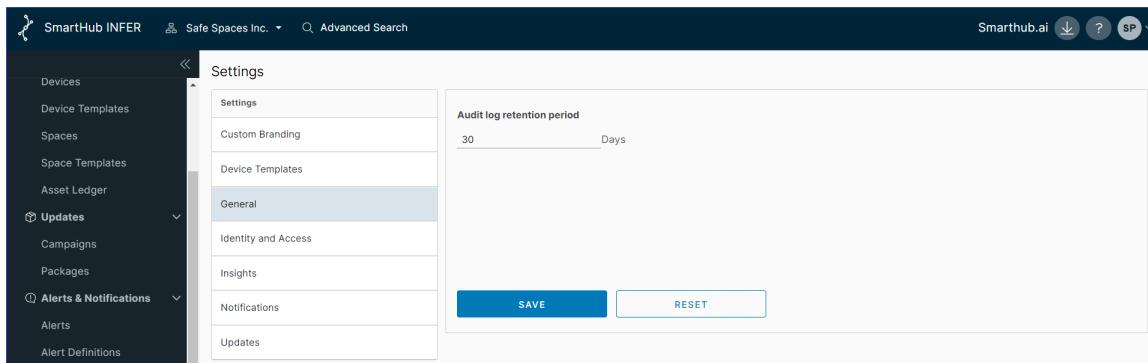
The Settings module in INFER™ allows you to define the audit log retention period for the organization.

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 INFER™. 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. From the INFER™ Console, go to **Settings > General**. This tab appears as shown below:



2. Under **Audit log retention period**, specify the number of days.
3. Click **SAVE**.
4. Click **RESET** to revert to default settings.

22.4 Setting up Identity & Access

The Settings module in INFER™ allows you to configure external identity provider (IdP) to authenticate access to INFER™ platform.

INFER™ uses IdPs as a third-party service to manage and authenticate user identities and provide Single Sign-On (SSO) capabilities.

- For more information on SAML authentication, see "Setting up SAML Authentication" below
- For more information on LDAP authentication, see "Setting up LDAP Authentication" on page 217

22.4.1 Setting up SAML Authentication

Security Assertion Markup Language (SAML) single sign-on (SSO) uses third-party authentication service providers to provide access to INFER™ 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. From the INFER™ Console, go to **Settings > Identity & Access**.
2. The **Enable external Identity Provider** switch appears ON by default.
3. Under **IDP Type**, **SAML** option in the drop-down 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.
 - 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 INFER™ metadata.



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 INFER™ for the particular 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 suborganizations. 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.
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™.

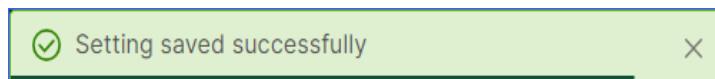
1. Click  to edit the attribute keys for creating the user, and click **DONE**.
2. Click  **+ Add** to add a new attribute keys for creating the user.
3. Click  to delete an existing key.



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™.

1. Click  to edit the group details of the user.
 2. Click  to delete an existing group.
 3. To add a new group for creating the user, click  **+ Add**.
 4. Under **Group Name**, enter the new group name.
 5. Next, under **Infer Group Name** select the desired groups from the drop down and click **DONE**.
16. Click **SAVE**. You have successfully configured the SAML SSO authentication settings in INFER™, and the following action confirmation message appears:



17. Click **RESET** to revert to default settings.

22.4.2 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 an 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:



- INFER™ is integrated with LDAP.



- LDAP is supported on on-premise versions of INFER™.

1. From the INFER™ Console, go 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.,
4. The **Just In Time user creation** switch appears ON by default, and allows all valid IdP users to login.
 - 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™, and the following action confirmation message appears:



16. Click **RESET** to revert to default settings.

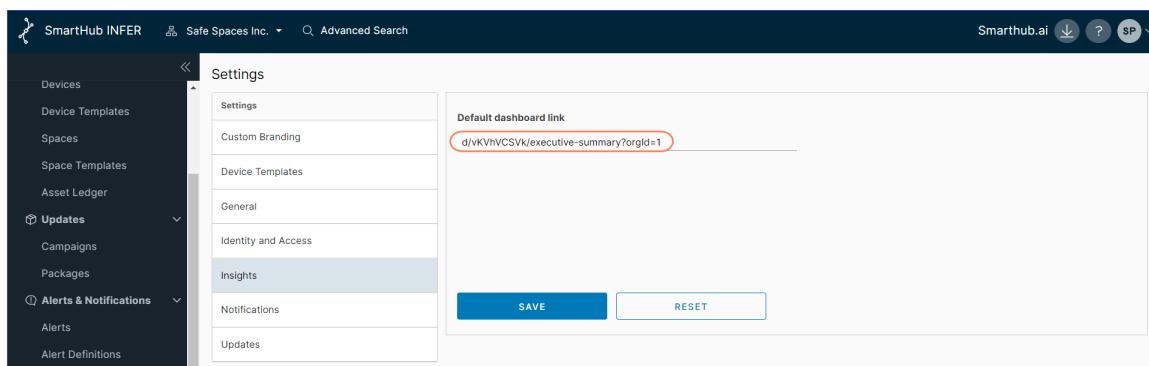
You can now log in to INFER™ Console with the external IdP credentials.

22.5 Setting up Insights Dashboard

The **Insights** module in INFER™ 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. From the INFER™ Console, go to **Settings > Insights**. This tab appears as shown below:


 A screenshot of the INFER™ Settings page. The top navigation bar shows "SmartHub INFER", "Safe Spaces Inc.", and "Advanced Search". On the right, there are icons for "SmartHub.ai", a download arrow, a question mark, and a "SP" dropdown. The left sidebar has sections for Devices, Device Templates, Spaces, Space Templates, Asset Ledger, Updates (Campaigns, Packages), and Alerts & Notifications (Alerts, Alert Definitions). The "Updates" section is currently expanded. The main content area has a sidebar titled "Settings" with options: Settings, Custom Branding, Device Templates, General, Identity and Access, Insights (which is highlighted in blue), Notifications, and Updates. Below this is a form field labeled "Default dashboard link" containing the URL "d/vKvhVCSVk/executive-summary?orgId=1". At the bottom are two buttons: "SAVE" (in blue) and "RESET". The overall interface is dark-themed.

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™, and the following action confirmation message appears:



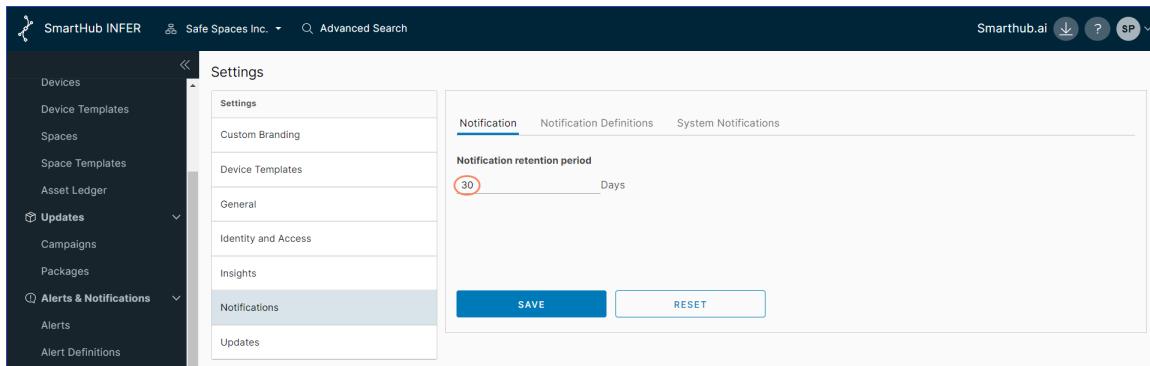
4. Click **RESET** to revert to default settings.

22.6 Setting up Notification Retention Period

The notification retention period refers to the duration for which INFER™ 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. From the INFER™ Console, go to **Settings > Notifications > Notification**. This tab appears as shown below:

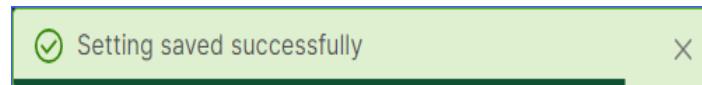


2. Under **Notification retention period**, specify the number of days.



The default notification retention period is 30 days.

3. Click **SAVE**. You have successfully set the notification retention period for your organization in INFER™, and the following action confirmation message appears:



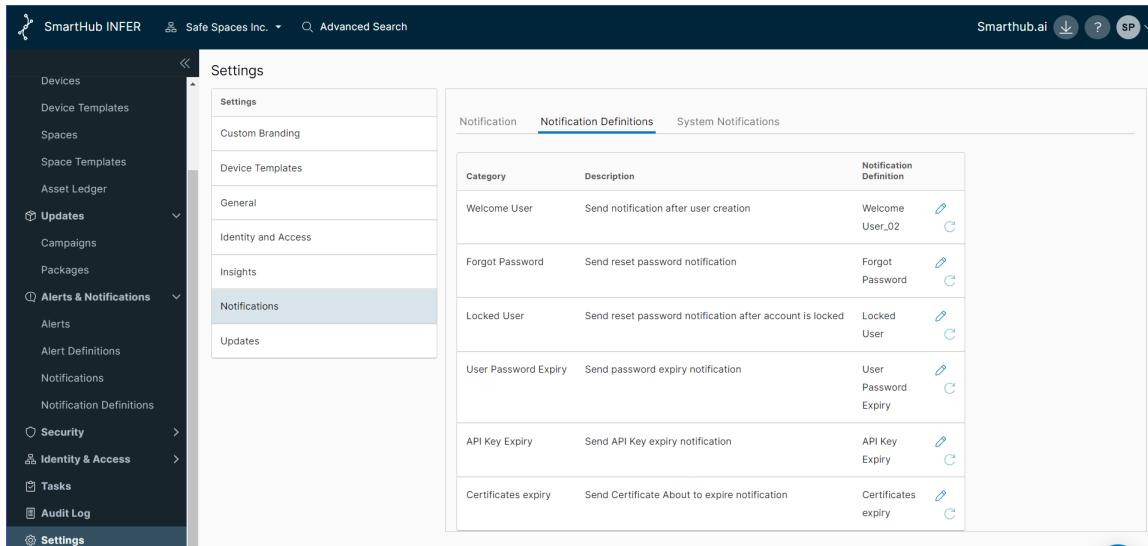
4. Click **RESET** to revert to default settings.

22.7 Setting up Notification Definitions

Notifications in INFER™ are email and REST 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?" on page 194.

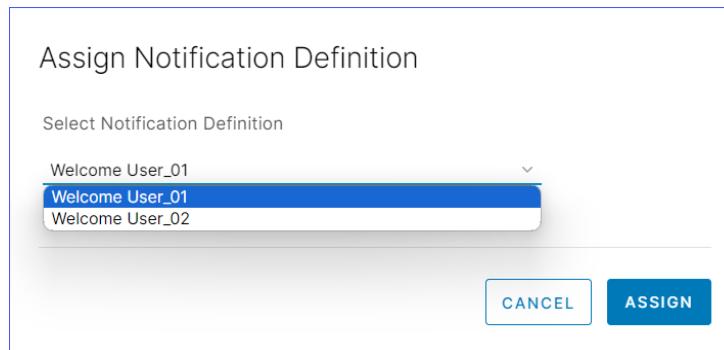
To edit the default notification definitions for your organization and all its sub-organizations, perform the following steps:

1. From the INFER™ Console, go to **Settings > Notifications > Notification Definitions**. The default list of notification definitions appears as shown below:



Category	Description	Notification Definition
Welcome User	Send notification after user creation	Welcome User_02  
Forgot Password	Send reset password notification	Forgot Password  
Locked User	Send reset password notification after account is locked	Locked User  
User Password Expiry	Send password expiry notification	User Password Expiry  
API Key Expiry	Send API Key expiry notification	API Key Expiry  
Certificates expiry	Send Certificate About to expire notification	Certificates expiry  

2. Under **Category**, click  to assign notification definition. The following pop-up appears as shown below:



3. Select the desired definition from the dropdown.
4. Click **ASSIGN**. The default notification category is updated.

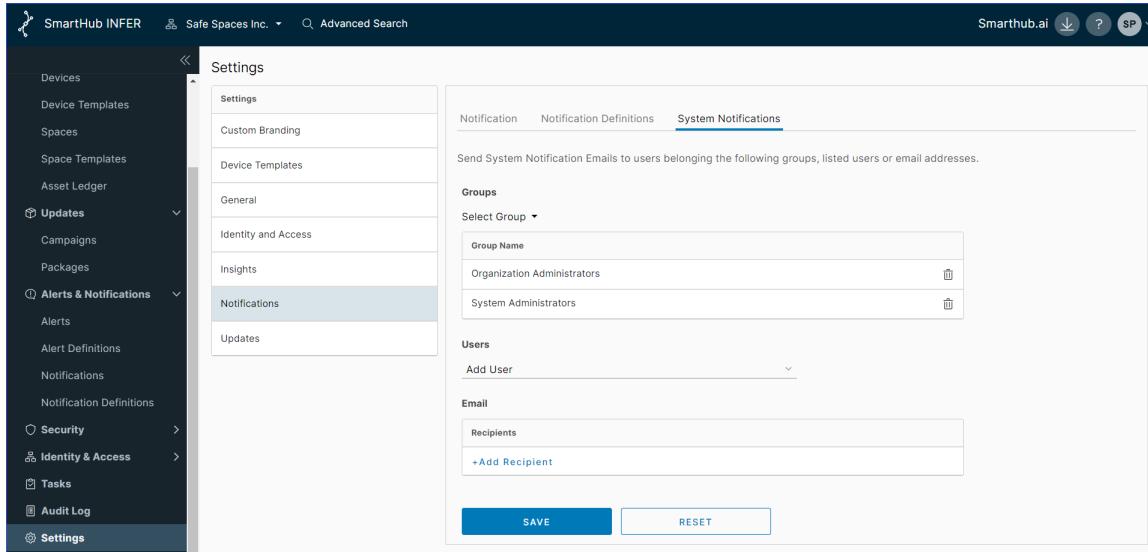
22.8 System Notifications Settings

System notifications in INFER™ are automated email messages generated based on predefined triggers or events to inform user groups, users, or email addresses of your

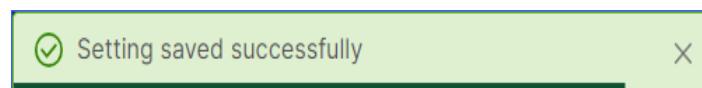
organization about important events or updates in INFER™.

To send system notification emails to users belonging to a particular group, listed users, or email addresses, perform the following steps:

1. From the INFER™ Console, go to **Settings > Notifications > System Notifications**. This tab appears as shown below:



2. Under **Groups**, click **Select Group** drop-down to select the required groups.
3. Under **Users**, add email IDs from the drop-down.
4. Under **Email**, add the recipient's email ID, and click **DONE**.
5. Click **+Add Recipient** to add another recipient.
6. Click **SAVE**. You have successfully created system notifications settings for your organization in INFER™, and the following action confirmation message appears:

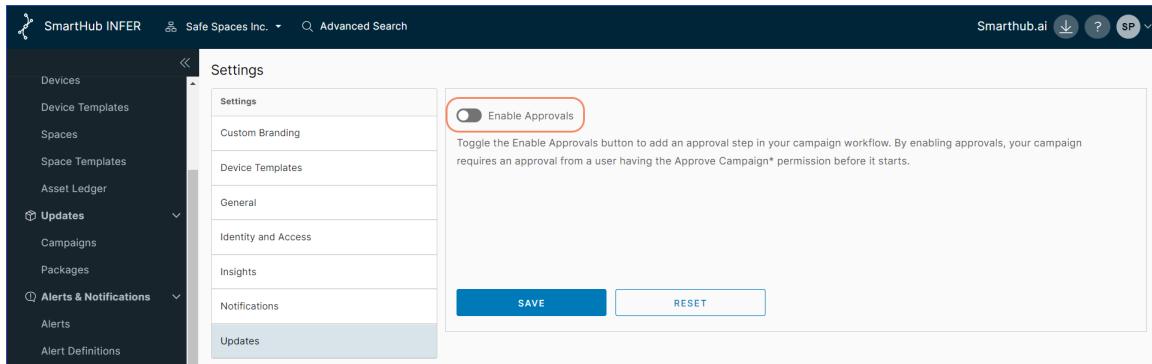


22.9 Setting up OTA Updates

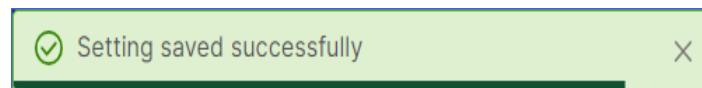
OTA updates eliminate the need for manual downloads making it easy for INFER™ users to keep their devices up to date.

To enable approvals for the OTA updates that are run in your sub-organizations, perform the following steps.

1. From the INFER™ Console, go to **Settings > Updates**. This tab appears as shown below:



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™, and the following action confirmation message appears:



4. Click **RESET** to revert to default settings.

23 Audit Logs

23.0.1 Viewing Logs

The **Audit Log** tab provides a view into the actions performed by all INFER™ users and devices.

You must have the VIEW_AUDIT_LOGS permission to perform this operation.

You can filter the audit logs based on the following parameters:

- Entity Type
- Audit Type
- Device
- Date Range

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**.

24 Tasks

The **Tasks** tab provides a view of all the tasks run by INFER™. It lists the tasks with the overall progress, user name, organization, and time of creation of the task.

You must have **View Tasks** permissions to perform this operation.

The Tasks tab displays basic information and entities of the device commands you send from INFER™.

1. To verify the basic information of a task, from the INFER™ 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), and name of the command run is displayed at the device level.

3. To view the progress of the command on each device, select **Entities**.

The list of devices on which the command is run is displayed. The status of the command such as completed, skipped, pending or failed is displayed against each device.

4. Click the **Device** name.

The Inventory - Device page is displayed.

5. To verify the progress of the command, click .. drop-down and select **Commands**.

Command history with the status is displayed.

25 TPM-Based Attestation

TPM-based attestation is a process to detect gateway tampering for file systems.

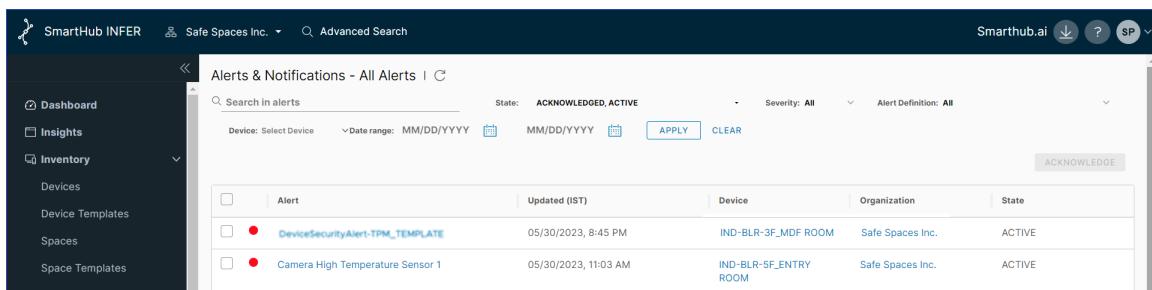
With the TPM-based attestation configured, INFER™ triggers an alert whenever a gateway is tampered.

TPM-based attestation are of two types:

- Boot Attestation
- Runtime Attestation

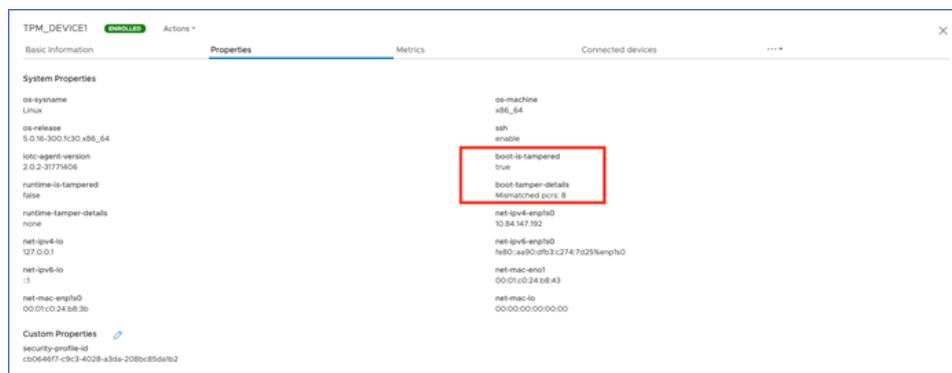
25.1 What is Boot Attestation?

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.



Alert	Updated (IST)	Device	Organization	State
DeviceSecurityAlert-TPM_TEMPLATE	05/30/2023, 8:45 PM	IND-BLR-3F_MDF ROOM	Safe Spaces Inc.	ACTIVE
Camera High Temperature Sensor 1	05/30/2023, 11:03 AM	IND-BLR-5F_ENTRY ROOM	Safe Spaces Inc.	ACTIVE

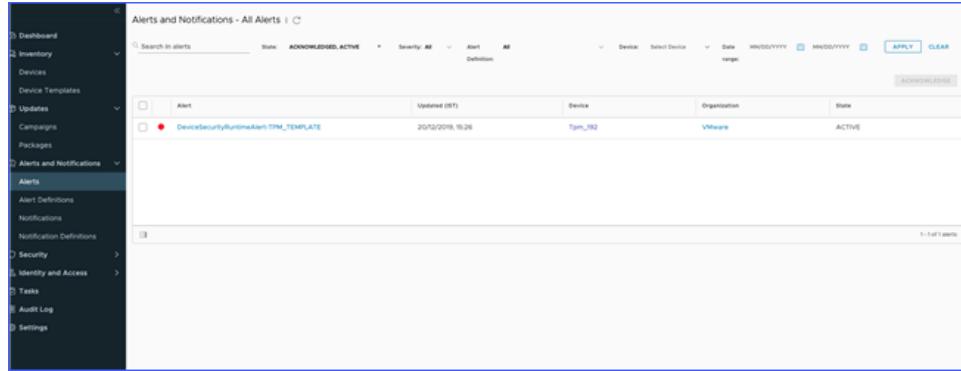
The cause of failure is updated in the gateway properties.



boot-tamper-details	Mismatched pcrrs: 8
---------------------	---------------------

25.2 What is Runtime Attestation?

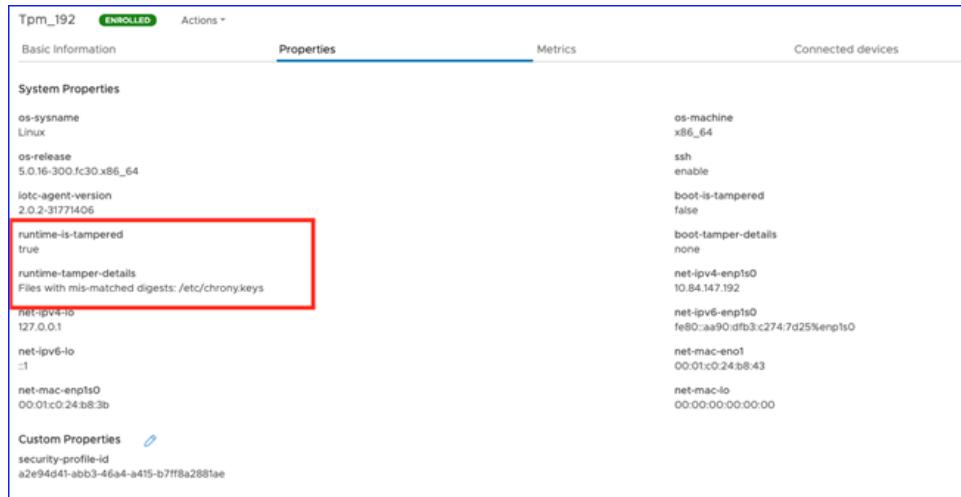
Runtime attestation is a secure mechanism to verify the integrity of an IoT gateway during run time. The runtime attestation check occurs every 3600 seconds. When a tampering is detected, INFER™ raises an alert.



The screenshot shows the 'Alerts and Notifications - All Alerts' page. The left sidebar includes sections like Dashboard, Inventory, Devices, Device Templates, Updates, Campaigns, Packages, Alerts and Notifications (selected), Alert Definitions, Notifications, Notification Definitions, Security, Identify and Access, Tasks, Audit Log, and Settings. The main area displays a table with one alert entry:

Alert	Updated (ST)	Device	Organization	Status
DeviceSecurityRuntimeAlert-TPM_TEMPLATE	20/02/2019, 19:26	Tpm_192	VMware	ACTIVE

The cause of failure is updated in the device properties.



The screenshot shows the 'Tpm_192' device properties page. The top bar shows 'ENROLLED' status. The page has tabs for Basic Information, Properties (selected), Metrics, and Connected devices. The Properties tab displays system and custom properties. A red box highlights the 'runtime-is-tampered' property, which is set to 'true'. Other properties listed include os-sysname, os-release, iotc-agent-version, net-ipv4-ip, net-ipv6-ip, net-mac-enp1s0, and security-profile-id.



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.

25.3 What Is IMA

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.

25.4 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.

25.5 Preparing Your Gateway for Runtime Attestation

For INFER™ to detect tampering, you must configure the following IMA settings on your gateway.

25.5.1 Configure 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=tcb ima_
policy=secure_boot ima_hash=sha256"
```

2. `sudo grub2-mkconfig -o /boot/efi/EFI/fedora/grub.cfg`.



These steps might not work with a Fedora IoT image.

Perform the following steps if the preceding steps do not work:

3. 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"
```

4. Restart the gateway for the settings to take effect.

25.5.2 Modify the */etc/fstab* File

Add the following line to the *fstab* file:

```
UUID=d4bbe97d-a719-43af-a89a-19a9455cec5b
/           ext4      noatime,iversion      1  1
```

25.5.3 Obtain 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.

25.6 Create a Boot Attestation Profile

Use the *fp.json* file to create a boot attestation profile in the INFER™ Console.

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. From the INFER™ Console, go to **Security > Profiles**.

2. Click **ADD PROFILE**.

The Add Profile wizard is displayed.

3. In the **Details** step:

1. Enter a profile name.

2. In the **Device 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 and Notifications > Alert Definitions**.

What to do next

Associate this profile with the TPM-based template.

25.7 Create a Runtime Attestation Profile

Use the *ima.json* and *fp.json* files to create a runtime attestation profile in the INFER™ Console.

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. From the INFER™ Console, go to **Security > Profiles**.
2. Click **ADD PROFILE**.

The Add Profile wizard is displayed.

3. In the **Details** step:
 1. Enter a profile name.
 2. In the **Device 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 **UPLOAD** and upload the *ima.json* file. Click **NEXT**.
Note: The maximum size allowed for uploading is 20 MB.
 6. In the **Review** step, 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 and Notifications > Alert Definitions**.

What to do next

Associate this profile with the TPM-based template.

25.8 Associate the Attestation Profile With the 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.

You must have a valid attestation profile.

1. From the INFER™ Console, go to **Security > Profiles**.
2. Copy the Profile ID of the attestation profile that you have created.
3. Go to **Device 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
```



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 device 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" on page 72.

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 device.



If there is a boot failure, the cause of the error is displayed. For example:

```
boot-is-tampered  
true  
boot-tamper-details:  
"PCR8 mismatched."
```

For a run-time failure, the cause of the error is displayed. For example:

```
runtime-is-tampered  
true  
runtime-tamper-details:  
"Files with mis-matched digests: /etc/chrony.conf"
```

25.9 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 IoT Package with a label added to the package-spec.yml file. For example:

```
# 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
```



The `security-profile-id: <label>` must match the security profile ID that you create in step 1.

3. Upload the package to INFER™. For information about uploading IoTC Packages, see "Working with Package Builder" on page 155.
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" on page 144.
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**.



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/activtcion.log 2>&1  
  
echo "Starting Activation for Updating Security Profile"  
>> /tmp/activtcion.log 2>&1  
  
  
sudo shutdown -r +1 >> /tmp/activtcion.log 2>&1  
  
  
echo 0
```



You have successfully applied a security profile across multiple gateway devices using campaigns.

26 Integrating with ServiceNow

You can integrate INFER™ with a ServiceNow instance.

INFER™ 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 INFER™ instance with ServiceNow.

You must have access to the following instances:

- INFER Console
- ServiceNow

1. Create a REST-based Notification Destination:

1. Log in to the INFER™ Console and navigate to **Settings > Notification Destinations**.
2. To create a notification destination, click **CREATE**.
The Create Destination wizard is displayed.
3. In the **Details** step, enter the name of your notification destination, an optional description, and click **NEXT**.
4. In the **Settings** step, enable **Secure Protocol**. Enter the Host URL of the ServiceNow instance. For example, dev79872.service-now.com. Enter the port number as 443.
5. Copy the security certificate from the ServiceNow browser and paste it in the **Certificate** text box.
6. Select the **Authentication Type** as **Basic** and enter your ServiceNow credentials in the **Username** and **Password** text boxes. Click **NEXT**.
7. In the **Review** step, review the details and click **SAVE**.

2. Create a Notification Definition:



1. Navigate to **Alerts and Notifications > Notification Definitions**.
2. In the **Alerts and Notifications - Notification Definitions** page, click **CREATE**.
The Create Definition wizard appears.
3. In the **Details** step, enter a name for the notification definition, enter an optional description, and click **NEXT**.
4. In the **Settings** step, select the **Type** as **REST Notification**, and select that destination that you created in step 1.



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.

5. In the URL field, append the URL with the path /api/now/table/incident.
6. Under **Advanced Settings**, add a new header with the header name as Content-Type. Enter the header value as application/json. Click **DONE**.
7. 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."  
}
```

```
}
```

8. Click **NEXT**.

3. Review the details that you have entered and click **SAVE**.

You have successfully integrated INFER™ with ServiceNow. When you associate an alert definition with this ServiceNow notification definition, ServiceNow files an incident whenever an alert is triggered.

27 Integrating with Third-Party CMS

To perform over-the-air software updates, operating system updates, and firmware updates to the gateways and devices 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 devices, use the **uploadProgram** API to integrate the CMS with INFER™.

For more information, see the *INFER™ API Reference Guide*.

28 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.

28.1 Troubleshooting Campaign Management

You can find troubleshooting steps for common campaign management problems in this section.

28.1.1 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` or `iotc-agent -f`.

28.1.2 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.

28.1.3 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.

28.1.4 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.

28.2 INFER™ Agent Connectivity to the INFER™ Server

When you onboard a gateway, at times, the devices are unable to connect to INFER™ Center and an error message is displayed. 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 device:

```
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 device: `/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 is displayed in the log file on the gateway device:

ERROR: GetCommand: HTTP GetCommand Request failed: ["Invalid Device token"]

4. If the preceding step fails, contact SmartHub Support.



If historical data associated with the gateway is not important, then you can try re-enrolling the gateway device. See "Onboarding Gateways" on page 63.